DIGITAL SIGNATURE CERTIFICATE CLASS -3

Q1: What is a digital signature?
A: Digital Signature is used to sign documents. DSC stands for "Digital Signature Certificate", also commonly known in short form as "Digital Signature".

Digital Signature is a software file. DSC can stored only in a special USB crypto token like ePass2003etc.

Q2: What is 'DSC'?
A: DSC is short for Digital Signature Certificate.

Q.3 What class of DSC should I buy?
DSC is now sold in only one class : Class-3. There will be no more Class-2 sold in 2021 as per CCA guidelines.
Class-3 DSC is sufficient to sign documents for a large variety of purposes - including tax returns (Income Tax /GST), invoice signing (Tally or PDF), completing Director's KYC, register new business firm on MCA Portal, applying Import Export Code (IEC), EPF Portal, etc.
Some Tender Portals require vendors to use Class-3 Digital Signature with encryption combo. Generally for tender bidders, Class-3 Combo is a safe recommended option.

Q.4 What is ePass2003 Auto token?

E Pass 2003 Auto is used to store Digital Signature Certificates. It is a secure storage device with strong authentication and password protected.

Designed to be secure from virus attacks, the token has mechanisms to prevent thefts of Digital Signature. E Pass 2003 Auto complies with the FIPS 140-2 security standards.

Q7: Can a digital signature be forged?
A: It is practically impossible to forge a digital signature. It is secure and has be applied online for authentication. Thus it is more secure than a hand-written signature which can

be seen and potentially imitated by any person who sees a document bearing the hand-written signature.

Q8: What is the validity of the digital signature?
A: You can choose to obtain a digital signature of 1 year or 2 year validity from date of issuance.

Q9: What happens after 1 year / 2 year?
A: After expiry of the validity period, the digital signature becomes invalid. You can then obtain a valid digital signature by following a simple procedure.

Q12. Where can you purchase a digital signature certificate?
A: Legally valid Digital Signature Certificates are issued only through a Controller of Certifying Authorities (CCA), Govt. of India,licensed Certifying Authorities (CA), a Certifying Authority (CA) licensed by CCA, offers secure digital signatures through various options tailored to suit individual as well as organizational needs.

Q13. Where can you use a Digital Signature Certificate?
A: You can use Digital Signature Certificates for the following:

- For sending and receiving digitally signed and encrypted emails.
- For carrying out secure web-based transactions, or to identify other participants of web-based transactions.
- In eTendering, eProcurement, MCA [for Registrar of Companies efiling], Income Tax [for efiling income tax returns] Applications and also in many other applications.
- For signing documents like MSWord, MSExcel and PDFs.
- Plays a pivotal role in creating a paperless office.

Q14. How does a Digital Signature Work?
A:A Digital Signature Certificate explicitly associates the identity of an individual/device with a pair of electronic keys - public and private keys - and this association is endorsed by the CA. The certificate contains information about a user's identity (for example, their

name, pincode, country, email address, the date the certificate was issued and the name of the Certifying Authority that issued it).

Q15.Can I use one Digital Signature Certificate for multiple E-mail Addresses?
A: No, you cannot. A digital signature certificate can have only one email address.

Q16.Can I use Digital Signature Certificate in e-tendering systems?
A: Digital signature certificates in e-tendering systems are allowed, but based on the service provider.

Q17.Can Digital Signature Certificates be used in wireless networks?
A: Yes, digital signature certificates can be employed in wireless networks.

Q18.What is a Certifying Authority (CA)?
A: A Certifying Authority is a trusted agency whose central responsibility is to issue, revoke, renew and provide directories for Digital Signature Certificates. According to Section 24 of the Information Technology Act 2000, "Certifying Authority" means a person who has been granted a license to issue Digital Signature Certificates.

Q19.Who can be a Certifying Authority?
A: The IT Act 2000 details the prerequisites of a CA. Accordingly, a prospective CA has to establish the required infrastructure, get it audited by the auditors appointed by the office of Controller of Certifying Authorities. Subsequent to complete compliance of all requirements, a license to operate as a Certifying Authority can be obtained. The license is issued by the Controller of Certifying Authorities, Ministry of Information Technology, and Government of India.

Q20.What is a Registration Authority (RA)?
A: A RA (Registration Authority) is an agent of the Certifying Authority who collects the application forms and related documents for Digital Signature Certificates, verifies the information submitted and approves or rejects the application based on the results of the verification process.

Q21.What is the role of CCA?

A: The Controller of Certifying Authorities (CCA) is a Government of India undertaking that license and regulate the working of Certifying Authorities. The CCA certifies the public keys of CAs, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose, CCA operates, the Root Certifying Authority of India (RCAI).

The CCA also maintains the National Repository of Digital Signature Certificate (NRDC), which contains all the certificates issued by all the CAs in the country.

Q22.What is NRDC?

A: In accordance with Section 20 of the IT Act, NRDC is a national repository maintained by the CCA that contains all Digital Signature Certificates and CRLs issued by all the licensed CAs. It also contains all the Digital Signature Certificates and CRLs issued by the CCA through its RCAI. All Relying Parties are allowed to verify the authenticity of a CA's public keys from this repository.

Q23.What is RCAI?

A: RCAI is the Root Certifying Authority of India. It was established by the CCA under Section 18(b) of the IT Act and is responsible for digitally signing the public keys of all the licensed CAs in the country.

The RCAI root certificate is the highest level of certification in the country. The RCAI root certificate is a self-signed certificate.

Q24.What is CRL?

A: The Certificate Revocation List (CRL) is a list of certificates that have been revoked by the CA, and are therefore no longer valid.

Q25.What is CPS?

A: The Certificate Practice Statement (CPS) is a statement of the practices that a Certification Authority (CA) employs for issuing and managing certificates. A CPS may take the form of a declaration by the CA of the details of its system's trustworthiness and the practices that it employs both in its operations and in its support of issuance of a certificate.

Q26. What is CP?

A: Certifying Authorities issue Digital Signature Certificates that are appropriate to specific purposes or applications. A Certificate Policy (CP) describes the different classes of certificates issued by the CA, the procedures governing their issuance and revocation and terms of usage of such certificates, besides information regarding the rules governing the different uses of these certificates.

Q27.What is Subscriber Agreement?

A: A Subscriber Agreement is an agreement between Subscriber and CA stating that the subscriber will use the Digital Signature Certificate for the assigned use or objective and that the subscriber is solely responsible for the protection of the private key and ensuring functionality of the unique key pair. The subscriber also agrees through the Subscriber Agreement that all the information provided to CA at the time of registration is accurate.

Q28. Why do I need to submit documents for a digital signature certificate?

A: A Digital Signature Certificate has almost the same importance in the digital world as your Passport or PAN card does in the physical world. Therefore, all information displayed on your Digital Signature Certificate needs to be verified before the certificate can be issued.

Q29.What is Certificate Revocation?

A: A Digital Signature Certificate can be revoked under circumstances such as the following:

- Users suspect compromise of certificate private key.
- Change of personal data.
- Change of relationship with the organization

Q30.Can someone other than the Subscriber revoke a certificate?

A: No, revocation is restricted to:

- The Subscriber in whose name the certificate has been issued.
- A duly authorized representative of the subscriber
- Authorized personnel of CA or RA when the subscriber has breached the agreement, regulation, or law that may be in force

Q31.How do I protect my Digital Signature Certificate/private key?
A:

- Protect your computer from unauthorized access by keeping it physically secure
- Use access control products or operating system protection features (such as a system password)
- Always protect your private key with a good password
- It is better download the digital signature certificate on to the crypto
- token which is more secure and tamper proof.

Q32.What do I do if someone copies my Digital Signature Certificate?
A**:** Your Digital Signature Certificate cannot be used without your private key. To maintain security, your private key should be protected by a password and never sent across any network. However, you do want your Digital Signature Certificate (which contains your public key) to be available to other users so that they can verify your right to use the Digital Signature Certificate, decrypt messages that you have encrypted with your private key, and verify your digital signatures.

Q35.I have forgetten my private key password. Can someone change it for me?
A: No. If you have forgotten your private key password, you will have to apply for a new Digital Signature Certificate.

Q36.I have lost the smart card/ USB Token containing my certificate and cryptographic keys. What do I do?

A: Please contact your nearest RA Administrator immediately to get your certificate suspended to avoid unauthorized access to it.

Q37.Will I Lose My Digital Signature Certificate if my Hard Drive is Formatted or Crashed?
A: If you have a soft token and if the hard drive is formatted or has crashed, the Digital Signature Certificate will be deleted.

Q38.I accidentally deleted my Digital Signature Certificate from my PC hard drive disk. What should I do now?
A: Once your Digital Signature Certificate and key files have been deleted, damaged or overwritten, there is no way to reactivate your Digital Signature Certificate. You need to revoke your Digital Signature Certificate and then enroll for a new one.

Q39.Why does a digital signature certificate have a limited validity period?
Ans. Digital signature certificates have an explicit start date and an explicit expiration date. Most applications check the validity period of a certificate when the digital certificate is used. The signature certificate expiration date is also used for managing the certificate revocation list (CRL). A certificate is removed from the revocation list when its natural expiration date arrives. As such, generally the shorter the certificate validity period, the shorter the CRL.

Q40. Can a person have two digital signatures say one for official use and other one for personal use?
Ans. Yes

Q41.Is Director Identification Number (DIN) a pre-requisite to apply for DSC?
A: No.

Q42. How much time do CAs take to issue a DSC?
A:The time taken by CAs to issue a DSC may vary from three to seven days.

Q43.What is Digital Time Stamping?

A: As the name suggests,a digital time -stamping service issues time- stamps. The function of Digital time stamp is similar to any other time stamp i.e. to denote date & time of an action on a document. Digital time-stamps are used to verify the original date of creation of a document.

- .Net Framework 4.5

Q45. Why do I need to validate a Digital Certificate?
A. Validation of a Digital Certificate is required to check the status of a digital certificate, to ensure that the digital certificate is valid for use and has not been revoked, changed or has expired.

Q46. What are Certificate Policies?
A. Certificate Policies describe details of different classes of certificates issued by a Certifying Authority. These details include procedures involved in the issuance and revocation of digital certificates and terms of usage of certificates.

Q47. Whether I am required to register myself as a Registered or Business user before registering DSC on MCA portal through the Register DSC facility?
A:No, user registration is not a pre-condition for registering the DSC through this facility on MCA portal. However, if you are a business user and had already registered your DSC earlier, then you are not required to register the same DSC through the Register DSC facility.

Q48. Who should register the DSC on MCA portal?
A:Directors, Manager and Secretary of the Company and practicing professionals i.e. CA, CS & CWA should register their DSC on MCA portal, if they have not registered their DSC as a business user earlier.

DIGITAL SIGNATURE CERTIFICATE CLASS -3

Q49. Why do I need to register my DSC on portal?
A:On registration of your DSC, MCA system shall capture the details of your DSC against your DIN/ PAN, as the case may be. This information will be used to authenticate your digital signature for role check purpose.

Q50. What will be the consequences if my DSC is not registered on the MCA portal?
A:Any eForm digitally signed by you for any Company being a director, manager, secretary or practicing professional, will not be accepted on the MCA portal once Role Check is implemented, as system will not recognize role associated with the digital signatures affixed on the eForm.

Q51. How do I register my DSC on MCA portal?
A:To register your DSC, select the "Register Digital Signature" link on the MCA Services and follow the given steps.

Q52. In Addition to MCA, where can I use my DSC?
A:Digital Signatures are legally admissible in a Court of Law, as provided under the provisions of Information Technologies Act, 2000. The acceptance of DSC is still not universal, however, various government authorities like Income Tax, GST etc have made it mandatory to use DSC for various applicants and it is voluntary for few exempted class. However, in near future it is expected to grow its presence and requirement with many other services.

Q53. I have a Class 3–Organisation DSC but I have left the organization, what should be done?
A:You have to apply for revocation of DSC.

Q54. Which class of Digital Signature is required for E Tendering?
A:A digital signature of Class 3 is required to perform E Tendering. However few sites may work on Class 2 Digital Signature as well. Further E Tenders also requires the Data

to be encrypted, so you will require an encryption certificate as well. Class 3 DSC are issued after rigorous verification process.

Q55. Do I need a PAN encrypted DSC for MCA filing?

A:No, PAN encrypted DSC is not mandatory for MCA filings. However you cannot use the same for Filing Returns on Income Tax Website if the DSC is not PAN encrypted.

Q56. I am a Proprietor, Partner and a Director, Do I need to buy Different DSC for every Filings?

A:No, you can use the same DSC for filing the returns of the Partnership Firm, Company. Suppose Mr. A is Partner in ABC Associates, Director in XYZ Ltd, Karta in ABC HUF and he also wants to file his own Individual Return. In this Case Mr. A is only required to take DSC in his Individual name and he can file the return of all entity with the same DSC.

Q57. Who all are required to obtain digital Signature Certificate (DSC) for Income Tax Filings?

A:Digital Signature Certificate (DSC) is mandatory for all assessee who are liable for audit u/s 44 AB of the Income Tax and all the Corporate assessee. Further Professionals like chartered Accountants who have to file audit reports & Certification on the Portal are required to obtain a Digital Signature Certificate. In case of other assessee’s DSC is not mandatory.

Q58. What is E Token?

A:An E Token is a smart card based USB device which is used for the Storage of you DSC.

Q59. Why do I require an E Token?

A:An E Tokens securely store your DSC with Strong passwords. Further it provides mobility to your DSC when you have to perform signing on multiple computers. You digital signature is Vulnerable to key Compromise if many users access the same machine on which you sign the documents with you DSC. However the same can be avoided with the help of an E Token.

Q60. I already have a DSC for Income Tax Filing; Can I use the same on MCA Portal?

A:Yes, you can use the same DSC on the MCA Portal.