Frequently Asked Questions (FAQs) on Digital Signature Certificates – Employers

Q:- What is a Digital Signature?

Ans:- A digital signature is an electronic form of a signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and also ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable and cannot be imitated by someone else. The ability to ensure that the original signed message arrived means that the sender cannot easily disclaim it later.

Q:- What is a Digital Signature Certificate (DSC)?

Ans:- Digital Signature Certificates (DSC) is the electronic format of physical or paper certificate like a driving License, passport etc. Certificates serve as proof of identity of an individual for a certain purpose; for example, a Passport identifies someone as a citizen of that country; who can legally travel to any country. Likewise, a Digital Signature Certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally.

Q:- Why do I need a Digital Signature Certificate?

Ans:- A Digital Signature Certificate authenticates your identity electronically. It also provides you with a high level of security for your online transactions by ensuring absolute privacy of the information exchanged using a Digital Signature Certificate. You can use certificates to encrypt information such that only the intended recipient can read it. You can digitally sign information to assure the recipient that it has not been changed in transit, and also verify your identity as the sender of the message.

Q:- Where can I purchase a Digital Signature Certificate?

Ans:- Legally valid Digital Signature Certificates are issued only through the Controller of Certifying Authorities (CCA), Govt. of India, licensed Certifying Authorities (CA), such as e-Mudhra, NIC, TCS, MTNL, n-code etc.

Q:- What is a Certifying Authority (CA)?

Ans:- 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.

Q:- What is the role of Controller of Certifying Authorities (CCA)?

Ans:- 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.

Q:- What purpose does the Digital Signature Certificates serve in the user's interaction with EPFO?

Ans:- As of now, the Digital Signature Certificates would be used for digital attestation of online claims and digital verification of member details in respect of claims submitted by members. Once submitted with digital attestation, there would be no need to submit the physical claims to EPFO office.

Q:- From Where I Can Purchase the DSC?

Ans:- You may check the following websites:

- www.safescrypt.com
- www.nic.in
- www.idrbtca.org.in
- www.tcs-ca.tcs.co.in
- www.mtnltrustline.com
- www.ncodesolutions.com
- www.e-Mudhra.com

Q:- What are the different classes of Digital Signature Certificates? Which class of Digital Signature Certificates is required for digital attestation/ verification in respect of EPFO?

Ans:- There are four classes of Digital Signature Certificates:-

Class 0 Certificate: Only for demonstration/ test purposes.

Class 1 Certificate: To individuals/private subscribers for E-Mail

Class 2 Certificate: These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.

Class 3 Certificate: This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.

It may be noted that only Class 2 or Class 3 Digital Signature Certificates would be needed for the work related to EPFO.

Q:- What User type should I select?

Ans:- You can select the 'User Type' based on your requirement of Digital Signature Certificate. It can be for personal, company or government use.

Q:- What 'Certificate Type' should I select?

Ans:- Based on requirement, you can select any one of these

- **Signature -** Certificate with this key usage, can be used for only digitally signing documents, emails and online transactions.
- **Encryption –** Certificate with this key usage, can be used for only encrypting documents, emails and online transactions.

Q:- What 'Type of Token' should I select?

Ans:- Based on requirement, you can select any one of these

- **Soft Token -** If you would like to download the Digital Signature Certificate to your local machine and use it from that specific machine only
- **USB Token -** If you would like to download the Digital Signature Certificate to a USB Token or a Smart card and use it from multiple machines

Q:- How does a Digital Signature Certificate work?

Ans:- 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).

These keys complement each other in that one does not function in the absence of the other. They are used by browsers and servers to encrypt and decrypt information regarding the identity of the certificate user during information exchange processes. The private key is stored on the user's computer hard disk or on an external device such as a token. The user retains control of the private key; it can only be used with the issued password.

The public key is disseminated with the encrypted information. The authentication process fails if either one of these keys in not available or do not match. This means that the encrypted data cannot be decrypted and therefore, is inaccessible to unauthorized parties.

Q:- Are Digital Signatures Certificate legally valid in India?

Ans:- Yes, as per Information Technology Act, 2000.

Q:- I have more than one authorized signatory. Whether I should purchase one Digital Signature Certificate (DSC) for all the authorized signatories or one Digital Signature Certificate (DSC) for each of the authorized signatories?

Ans:- If you have more than one authorized signatory, then you have to purchase one Digital Signature Certificate (DSC) for each of the authorized signatories and register each of them on Online Transfer Claim Portal (OTCP) of EPFO separately.

Q:- While registering the Digital Signature Certificate on the OTCP portal of EPFO, I have come across the error: "Invalid certification chain received". The Certifying Authority (CA) has confirmed that there is no problem with DSC. How can I handle this error?

Ans:- With respect to the "Certification Chain" error being received, there is a possibility that the DSC has been incorrectly installed on the computer. Before using a DSC, the certificate trust chain of the issuing authority needs to be installed. If this certificate chain is missing, the above error is received. Thus the owner of certificate needs to install the root and intermediate certificates explicitly.

An example for TCS is given on page 10 of this document available on the link https://www.tcs-ca.tcs.co.in/pdf/Vista_Windows7_Enrollment_Procedure.pdf. Further it may be noted that in order to verify the DSC, the presence of certification chain is must. This is supported by the document at the link http://www.mca.gov.in/MCA21/pdf/TroubleshootingErrorsWhileUsingDSC.pdf.