FAQs on DSC.

A) What type of certificates is required to access EPS ?

PGCIL Version is PKI enabled & DSC is required to access the site. The specifications for the same are Class III SHA 2 2048 bit. One certificate is for signing and other one for Encryption.

B) What is the validity of a certificate?

Certificates are valid for two years from date of issue.

C) Is the DSC renewed?

No Certificates are not renewed, though some service providers may term it as renewal, the fact is a new certificate is issued with a fresh algorithm. Algorithm cannot and will never be the same is two certificates.

D) Can I use an expired certificate?

- Signing Certificate: On expiry it will not be usable. The PKI Component will not allow to login with an expired signing certificate. Hence with an expired signing certificate you will not be able to do any activity.
- Encryption Certificate: Expired certificates will be required for decryption in case a bid copy is created out of such sign # and present in user system, but cannot be used for encryption.

E) Do I need to retain the expired certificate?

Yes, Especially the Encryption Certificate. Else you may not be able to decrypt the bid. Wise decision would be to retain both.

F) My certificates expired and reside in a USB e-Token? What should I ensure?

USB e-Token can accommodate upto 8 certificates. Hence when you give the USB e-Token to your service provider for obtaining new certificate, you should ensure that your service provider does not delete the existing certificate or overwrite the existing certificate. You may also request your service provider to provide certificates in a new e-Token to avoid any loss.

G) My certificates expired and but these were installed in the browser vide the .pfx/.p12 file, I have accidentally deleted this, What should I do

You should never delete the certificates. In case you have accidentally deleted it, please reinstall the same again in browser. Expired certificates can be re-installed again from .pfx/.p12 files. Hence **NEVER** lose the .pfx/.p12 files and also the password to install the same.

NB: Sale of .Pfx/p12 files have been banned by DiT. Some users may still having the .pfx files, which are due to be expired. Hence CAs will issue new certificate only vide USB tokens.

FAQs on DSC.

H) Should I wait till expiry to apply for new certificates?

You should ideally start processing for the new atleast 1 (one) month in advance before expiry. This will avoid time lag.

I) My Certificates will be expiring in coming days, but I already obtained both new Signing and Encryption DSCs. What should I do?

This scenario is considered to be the ideal scenario and is best proactive practice. In this case, you need to do the following, immediately on obtaining both the new certificates.

1) User can log in to the system with his current Signing DSC
2) Click "Digital Certificate"
3) Select ADD certificate
4) Map the new certificates for signing as well as encryption.

Alternatively, the mapping can be also done from the certificate information page that is displayed immediately after login.

J) My Certificates have expired, but I have the new DSCs or will obtain new certificates soon. What should I do next?

Firstly, you should immediately approach your DSC service provider and procure the same.

Secondly, since you will not be able to log in with expired certificate, You should immediately inform Mjunction Helpdesk team immediately to deactivate the expired Signing certificate.

Thirdly, once the Mjunction Helpdesk team de-activates your expired signing certificate, you would need to map your new certificate (as you had done during your first ever login) again.

Fourthly, Mjunction Helpdesk team will to approve the same, post which you can login.

NB: For mapping Encryption Certificate you can map it yourself once you are able to login to the site (as you had done before).

K) I am the Administrator. One of the users certificate has expired. He has requested me to deactivate the expired certificate. What should I do?

As an Administrator, you should only de-activate the expired signing certificate of the user.

At no point in time you will de-activate the Encryption certificate; else user will face issues during decryption with expired Encryption certificate.

This will enable the user to map his new signing certificate, which you will have approve, as you would be doing for any new user.

L) As an administrator or SPoC for EPS of PGCIL, what should I be advising my users? When should I take necessary steps.

Being the Administrator or SPoC, you are the one who has full information of expiry of DSCs of all users. The data is available to you from the EPS portal. Further you may already have this information as an SPoC, as you may have initiated bulk purchases in the past. This enables you to act in advance and plan things accordingly to avoid any hassles.

1) You can proactively inform all buyers (and suppliers also) on the above points.
2) You can request your buyers to inform the suppliers.
3) You can initiate bulk purchases, in advance. This would also have an negative impact on your cost or procurement of DSCs.

M) Can I Map more than 1 DSC set (Signing & Encryption) against my one user id?

Yes. For clarity please refer to example below:

Say "ABC" is user id in PGCIL and a DSC set SC1 and EC1 (SC= Signing Certificate, EC= Encryption Certificate) is already mapped to it. In this scenario SC1 and EC1 cannot be mapped to any other user id in PGCIL

However SC2 and EC2 can be also mapped to user id "ABC" in PGCIL, provided SC2 and EC2 is free, i.e these are not mapped to any other user id in PGCIL. If the same is visibly mapped to say user id "XYZ" in PGCIL then the same cannot be mapped to "ABC" in PGCIL.

Hence more than 1 certificate can be mapped against one user id provided the certificates are not being used in any other user id in the same organization. In other sense multiple userids cannot be mapped to one certificate in the same organization.

To map SC2 and EC2, User will login with "ABC" using SC1 certificate and then in the first page or the Digital certificate list page, the user can map the new certificate, by clicking the register certificate.

N) When Should I handover back the DSCs to my organization.

During Retirement, Transfer, or in case of resignation, DSCs should be handed back to organization as it is organization or company's property, because certificates are issued to individual to act on behalf of the company.
The certificates should not be ethically used by you as in case of retirement, Transfer or resignation, you are not authorised to use the certificate in such a scenario.