



रक्षालेखाप्रधाननियंत्रक (प.क.), चंडीगढ़
PRINCIPAL CONTROLLER OF DEFENCE ACCOUNTS (WC),
Sector-9, Chandigarh-160009
Tel No: EPABX Nos:2741611-614,2741990,2740445, Ext: 286, 280
Fax – 2742552 E-mail: pcdawcits.dad@hub.nic.in
Website: pcdawc.gov.in



6834

IT&S/Cell/1367/Raksha Awas/Vol-II

Date: 15 /09/2020

Important Circular

To

The Officer Incharge

- 1) All Section in Main Office
- 2) All Sub Offices under PCDA (WC) Chandigarh.

Sub: - DSCs (Digital Signature Certificate): Guidelines thereof

Ref: - HQrs Office letter No. IT&/714/Bhawan Portal dated 26-05-2020

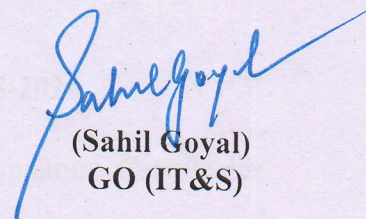
This office is in process of procuring and issuing Digital Signature Certificates (DSCs) to staff and officers of Main Office as well as Sub-offices under the jurisdiction of PCDA (WC) Chandigarh for implementation of various ongoing IT Projects in the department. In this regard following Instructions are issued for its usage and compliance by all officers in charge:

- (1) Officer In charge of every section in of M.O. as well as Sub-office may ensure to open a register and take stock of every Digital Signature Certificates (DSC) whenever issued to staff and Officers.
- (2) As part of handing over of charge of given officer, the DSC issued to the officer be revoked. Further, his user credentials in the respective applications should be deactivated so that he can no longer access the application while the Certificate revocation is under process with the CA (Certifying Authority). Once the DSC is successfully revoked, the officer will be no longer able to sign the documents.
- (3) Digital Signature Certificates are issued with a planned lifetime, which is defined through a validity start date and an expiration date. Once issued a Certificate is valid until its expiration date. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include change of name (for example change the subject of a certificate due to an employee's change of name), change of association between subject and CA (for

example, when an employee terminates employment with an organization, transfer, Superannuation), and compromise or suspected compromise of the corresponding private key. Under such circumstances, the issuing CA needs to be contacted for revoking the certificate.

- (4) In case, a Digital Signature Certificate is compromised, all officer-in-charge should immediately contact the Main office/respective CA to initiate revocation. The CA will then put the certificate in the Certificate Revocation List.

Please acknowledgement receipt.



(Sahil Goyal)
GO (IT&S)

Copy to:-

The OI/C

IT&S

(Local) : for uploading on website.


(Ankit Sud)
AO (IT & S)