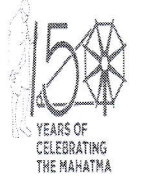




कार्यालय ,रक्षा लेखा नियंत्रक
नं. 1स्टाफ रोड, सिकिंद्राबाद ,
Office of the Controller Of Defence Accounts
No.1 Staff Road, Secunderabad-500 009
(Tele/Fax:040-27843385/27847957 Fax: 040-27810499)
Email id: cda-secd@nic.in



ITS/GenCorr/DigitalSignature

Dated: 03.06.2020

To

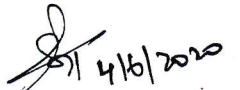
1. The DCDA I/c, PAO (ORs) EME, Sec'bad
2. The DCDA I/c, AAO (Army), Vizag
3. The ACDA I/c, PAO (ORs) AOC, Sec'bad
4. All SAOs / AOs & All sections in Main Office (Local)
5. All sub-offices located at Sec'bad/Hyd/Vizag/Eddumailaram/Suryalanka.

Subject: Digital signature Certificates for various projects in the department

Reference: Hqrs office lr. No. IT&S/714/Bhawan Portal dated 26.05.2020

Attention is invited to Hqrs letter cited under reference which is also available in CDA Sec'bad website i.e. cdasecbad.ap.nic.in and IT Helpline of CDA Sec'bad. Requirements, if any, of Digital signature Certificates may be forwarded with approval of respective competent authority along with all supporting documents to IT Section of this office for further necessary action. The contents of the letter may be strictly complied with before forwarding requirement.

It is also requested to intimate the details of Digital signature Certificate, if already available with your office, mentioning name of the person, type of key, validity etc.,


(S SRINIVAS)
ACDA (ITS)

 <p>सत्यमेव जयते</p>	<p>भारत सरकार रक्षा मंत्रालय Government of India Ministry of Defence रक्षा लेखा महानियंत्रक Controller General of Defence Accounts उलान बटार रोड, पालम, दिल्ली छावनी-110010 Ulan Batar Road, Palam, Delhi Cantt - 110010 Ph- 011-25665863,25665763 , Fax- 011-25675030 Email: cgdanewdelhi@nic.in</p>	 <p>सत्यमेव जयते रक्षा लेखा विभाग DEFENCE DEPARTMENT ACCOUNTS</p>
IT&S WING		
IT&S/714/Bhawan Portal		dated 26-05-2020

To,

All PCsDA/CsDA/PCA(Fys)/PIFAs/IFAs

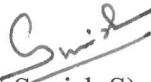
Sub: Digital Signature Certificates for various projects in the department

This office has received various references with regard to procurement and implementation of Digital Signature Certificates for various IT projects in the department.

2. In this context the following instructions/clarifications are issued:
- a) The Digital Signature Certificates for official use may be procured by the respective controller offices on need basis for its users.
 - b) Digital Signature Certificates for organizational use should be procured in compliance with the identity verification guidelines issued by CCA, MeiTY available at <http://www.cca.gov.in/sites/files/pdf/guidelines/CCA-IVG.pdf> as amended from time to time.
 - c) All procurements may be made from the IT funds allotted to the respective controllers. The procedure of purchases may be regulated as per extant rules and regulations prescribed under GFR and other relevant orders.
 - d) It is recommended that as part of the handing over of charge of a 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.

- e) Digital Signature Certificates are issued with a planned lifetime, which is defined through a validity start date and an explicit expiration date. A certificate may be issued with a validity of up to two years. 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.
- f) In case a Digital Signature Certificate is compromised, PCsDA/CsDA should immediately contact the respective CA to initiate revocation. The CA will then put the certificate in the Certificate Revocation List.
- g) PCsDA/CsDA need to have necessary processes in place defining the roles and responsibility of various government officials for the usage of Digital Signature and their revocation.

This issues with the approval of Addl. CGDA (IT&S).


(Dr. Sunish S)
Dy. CGDA (IT&S)