KEEP YOUR DIGITAL SIGNATURE KEY SECURELY, DO NOT SHARE IT WITH ANY ONE.

DIGITAL SIGNATURE is equivalent to handwritten signatures

DO'S AND DON'TS

- Email id included in the application should solely be in the control of the applicant.
- For Class 2 & 3 Digital Signature Certificates (DSC), the digital signature key should be generated and stored on a complient hardware cryptographic device.
- Strong password should be used to protect the digital signature key in the cryptographic device. The password should not be shared with anyone.
- Before accepting the DSC from the issuing Certifying Authority(CA), ensure that information given in the application is correctly included in the DSC.
- In case of loss or compromise of the cryptographic device, the CA who has issued the DSC must be informed immediately.
- Read the DSC Subscriber obligations which are part of the Certification Practice Statement (CPS) published on the website of CA.

davp 06108/13/0005/1516

GOVERNMENT OF INDIA
Ministry Of Communications and Information Technology
Department of Electronics & Information Technology

CONTROLLER OF CERTIFYING AUTHORITIES

CONTROLLER OF CERTIFYING AUTHORITIES
6, CGO Complex, Electronics Niketan
Lodhi Road, New Delhi - 110003
E-mail : info@cca.gov.in Website : http://cca.gov.in

Hindustan Times, New Delhi, 17th Oct 2015