NIC Certifying Authority
National Informatics Centre
Ministry of Communications and Information Technology
Government of India

Ref. No. ....
(To be filled by NICCA)

DIGITAL SIGNATURE CERTIFICATE REQUEST FORM

NOTE:

Affix Recent
Passport Size
Photograph

1. This application form is to be filled by the applicant.
2. Please fill the form in BLOCK LETTERS.
3. Please Tick (√) the appropriate option.
4. All subscribers are advised to read Certificate Practice Statement of CA.
5. Incomplete/Inconsistent applications are liable to be rejected.
6. Validity period should not exceed the date of superannuation of the applicant.
7. Asterisk (*) marked entries should not be left blank as these are reflected in the Digital Signature Certificate.

1. Category of Applicant : Government / Judiciary / PSU & Statutory Bodies / Registered Companies

2. Class of Certificate Required **(see pt. 11 at page 4)** : Class I / Class II / Class III

3. Certificate Required (Usage) **(see pt. 11 at page 4)** : Individual (Signing) / Encryption / SSL Server

4. Certificate Validity **(Max. 2 Years)** : Two years / Specify validity (if less than 2 years) _____

5. Date of superannuation* (dd/mm/yyyy) : _____

6. Name* : _____
   (First Name)   (Middle Name)   (Last Name)

7. Designation : _____

8. Email ID* (Official email-ID preferred) : _____

9. Ministry/Department : _____

   a) Office Address : _____
   _____
   Telephone (Official)_____(Resi/Mobile) _____

   b) Residential Address : _____
   _____

10. Identification Details (Tick any one) : _____
   [Employee ID / Passport No. / PAN Card No. / Voter ID
   Card No. / Driving License No. / PF No. /Bank Account
   Details /Ration Card No.] _____

11. **Certificate Subject Details*** : **Organization*** _____
   (These will be used in Certificate subject.) **Organization Unit*** _____
   City* _____
   State* _____
   Country*   **INDIA**

12. SSL Certificate Details : Web Server _____
   (In case the application is for a device then details of Services _____
   Server/Device for which the certificate is being applied IP Address _____
   for must be filled.) URL/Domain Name _____
   Physical Location _____

Date: ....
Place: ....

....
(Signature of the Applicant)

(For NICCA Office use only)

Smart Card/USB Token Sr. No.:........................

Authorised Signatory / RAA:

Name : ....

Date: ....

Request No : ....
RA Code : ....

Remarks: ....

Declaration by the Subscriber

I hereby declare and understand that

1. I have read the subscriber agreement under Resources (https://nicca.nic.in).
2. I shall keep the private key safe and will not share with others.
3. I shall verify the contents and the correctness of the certificate before accepting the DSC.
4. I shall send a signed mail to NIC-CA (support@camail.nic.in) to acknowledge the acceptance of the DSC.
    I also undertake to sign an additional declaration form in case of Encryption Certificate.
5. I shall not use the private key before acceptance of the DSC.
6. I authorize NIC-CA to publish the certificate in the NIC-CA repository after acceptance of the DSC.
7. If the private key of my DSC is compromised, I shall communicate to NICCA without any delay as per requirement mentioned in Regulation 6 of Information Technology (Certifying Authority) Regulations, 2001. (Doc ID CA2-50027.pdf, available under Repository>CPS & Forms>All Forms at https://nicca.nic.in)
8. I understand the terms and conditions of issued DSC and will use the DSC under the terms of issue as in the Certificate Practice Statement.
9. I understand that on cessation of my employment, I shall inform NICCA and my present employer for revocation of my Digital Signature Certificate.
10. I certify the following: *(Tick whichever is applicable)*
    o I have not applied for a DSC with NIC-CA earlier.
    o I have been issued a DSC by NICCA with User ID _____which is Valid/Revoked/Suspended/Expired.

The information furnished above is true to the best of my knowledge and belief. I will comply with the terms and conditions of Subscriber (as in section 40-42 of the IT Act 2000) and those of the Certificate Practice Statement of the NIC-CA. If at a later stage any information is found to be incorrect or there is non-compliance of the terms and conditions of use of the DSC, NIC-CA will not be responsible for the consequences/ liabilities and will be free to take any action including cancellation of the DSC.

Date : ....
Place : ....

....
(Signature of the Applicant)

Verification and Declaration by Head of Office of Applicant

1. This is to certify that Mr./Ms _____has provided correct information in the Application form for issue of Digital Signature Certificate for subscriber to the best of my knowledge and belief. I have verified the credential of the applicant as per the records and the **guidelines given at page 5.** I hereby authorize him/her, on behalf of my organization to apply for obtaining DSC from NICCA for the purpose as specified at point 3 of page-1.

2. It is noted that the organization shall inform NICCA for revocation of DSC on the cessation/superannuation of his/her employement.

Date : ....
Place : ....
Office Email:

(Signature of Officer with stamp of Org./Office)
Name of Officer with Designation:

Forwarded by SIO / NIC Coordinator
(Only for Class-2 & Class-3 Certificate)

(Signature of SIO /NIC Coordinator)
Name: ....
Date: ....
Office Seal:

This form is to be forwarded to the respective RA Office of NIC-CA.

Additional Declaration by the Subscriber for Encryption Certificate

I hereby declare and understand that

1. I am solely responsible for the usage of these Certificates/Tokens/ Technology. I shall not hold NICCA responsible for any data loss/damage, arising from the usage of the same.
2. I am aware that Key Escrow/Key Archiving of Encryption keys is not done by NICCA and I shall not hold NICCA responsible or approach NICCA for recovery of my private Encryption Key, in case of its loss or otherwise.
3. I shall be responsible for compliance to the relevant sections of the IT Act/Indian Telegraphic Act and other Acts/laws of the Indian legal system, pertaining to Encryption/Decryption of any message or document or electronic data, and I shall be liable for associated penal actions, for any breaches thereof.
4. NICCA shall not be held responsible and no legal proceedings shall be taken against NICCA for any loss and damage that may occur due to any reason whatsoever including technology upgradation, malfunctioning or partial functioning of the software, USB token, Smart Card or any other system component.
5. I am aware that the Encryption Certificate, issued by NICCA is valid only for the suggested usage and for the period mentioned in the certificate. I undertake not to use the Certificate for any other purpose.
6. I am conversant with PKI technology, and understand the underlying risks and obligations involved in usage of Encryption Certificate.
7. I certify the following: *(Tick whichever is applicable)*
   - I have not applied for an Encryption Certificate with NIC-CA earlier.
   - I have been issued an Encryption Certificate by NICCA with User ID _____which is Valid/Revoked/Suspended/Expired.

The information furnished above is true to the best of my knowledge and belief. I will comply with the terms and conditions of Subscriber (as in section 40-42 of the IT Act 2000) and those of the Certificate Practice Statement of the NIC-CA. If at a later stage any information is found to be incorrect or there is non-compliance of the terms and conditions of use of the Encryption Certificate, NIC-CA will not be responsible for the consequences/ liabilities and will be free to take any action including cancellation of the Encryption Certificate.

Date : ....
Place : ....

....
(Signature of the Applicant)

Declaration by Head of Office of Applicant

I hereby authorize Mr/Ms _____ employed in this Organization, to apply for Encryption Certificate from NIC-CA. It is further certified that a Policy/Procedure is in place, which describes the complete process for Encryption Key Pair Generation, Backup Procedure, safe-keeping of Backups and associated Key Recovery Procedures. The consequences of loss of the key have been explained to the user and he/she has been advised about securing the key and making it available to relevant authorities, in case of emergency.

Date : ....
Place : ....

(Signature of Officer with stamp of Org./Office)
Name of Officer with Designation:

Office Email:

Forwarded by SIO / NIC Coordinator
(Only for Class-2 & Class-3 Certificate)

(Signature of SIO /NIC Coordinator)
Name: ....
Date: ....
Office Seal:

This form is to be forwarded to the respective RA Office of NIC-CA.

Instructions for DSC Applicants

1. NIC-CA abides by the Information Technology Act, 2000, laid down by the Govt. of India. The applicant is advised to read this IT Act 2000 under Resources (https://nicca.nic.in).
2. To use DSC for exchanging Digitally signed Email, S/MIME compatible Mail clients should be used (Outlook Express, etc.). Also, please ensure that your email-id is issued from a POP compatible Mail server. For security reasons, NICCA prefers usage of Official E-mail ID.
3. Subscriber is required to send one copy of DSC request form, duly signed and forwarded by Head of Office. Applicant is advised to retain a copy of the same, for filling up the form online while generating key-pair.
4. The forwarded DSC application form is processed at NIC-CA for issue of DSC. If all particulars are in order, a User-Id, password and the profile for the applicant is created using the details submitted. This user-id will only be valid for 90 days (i.e., applicant has to generate key pair request and download certificate within 90 days) failing which, user is required to submit fresh DSC application for DSC issuance.
5. It is very important to keep the private key securely.
6. If the private key is compromised, applicant should immediately inform NIC-CA office by phone 011-24366176 or e-mail at support@camail.nic.in and Login with his user-Id and password at NIC-CA website. The User has to send Request for Revocation/Suspension/Activation form (CA2-50027.pdf)
7. For viewing all valid DSCs and CRLs, the user can access the website (https://nicca.nic.in/) under Repository.
8. DSCs are normally issued on FIPS-140 Level-2 compliant smart card/USB crypto-tokens, **which allows only maximum ten numbers of incorrect attempts for entering pass phrase/ pin**. It is advisable to be careful while entering the passphrase as repeated incorrect entries may block the same. On exceeding this limit, special efforts may be required to unblock the device.
9. It is important to note that email-id given by the applicant is functional and applicant accesses the same on regular basis as all communications w.r.t DSC like generation, revocation, renewal, expiry details are communicated through the given email-id.
10. For any further clarification, user can write to support@camail.nic.in or visit the NIC-CA website (https://nicca.nic.in).
11. ***Types of Classes: Depending upon requirement of assurance level and usage of DSC as described below, the applicant may select one of the classes.***
    Class-1 Certificate:
    Assurance Level: Provides minimum level of assurance. Subscriber's identity is proved only with help of Distinguished Name –DN and hence provides limited assurance of the identity.
    Suggested Usage: Signing certificate primarily be used for signing personal emails and encryption certificate is to be used for encrypting digital emails and SSL certificate is used to establish secure communications through the use of secure socket layer (SSL).
    Category Issued to the Individual from Govt., PSU/Statutory Bodies, Government Registered Companies and Web Servers/Servers within NIC domain
    Class-2 Certificate:
    Assurance Level: Provides higher level of assurance confirming the details submitted in the DSC Request Form, including photograph and documentary proof in respect of at least one of the identification details.
    Suggested Usage: In addition to the 'suggested usage' mentioned in class I, the class II Signing certificate may also be used for digital signing, code signing, authentication for VPN Client, web form signing, user authentication, Smart Card Logon, single sign-on and signing involved in e-procurement/ e-governance applications.
    Category Issued to the Individual from Govt., PSU/Statutory Bodies, Government Registered Companies and Web Servers/Servers in open domain.
    Class-3 Certificate:
    Assurance Level: Provides highest level of assurances, as verification process is very stringent. Proves existence of name of organizations such as Government Departments/Agencies, PSU/ Govt. Registered Companies and assures applicant's identity authorized to act on behalf of the Government/PSU/Statutory/Autonomous bodies/ Government registered Companies.
    Suggested Usage: In addition to the 'suggested usage' mentioned in class-1 & class-2, class-3 signing certificate may also be used for digital signing for discharging his/her duties as per official designation. Class-3 encryption certificate may also be used for encryption requirement as per his/her official capacity.
    Category Issued to individuals from Government entities/Head of the Institutions, Statutory/Autonomous bodies, Government registered Companies

Guidelines for verification by Head of Office

- The Head of Office (HO) of DSC requestor has to verify the identity /credentials of applicants. They will be solely responsible for authentication and validation of each subscriber/applicant within the organisation.
- They have to ensure verification process as described below, depending upon the class of certificate as applied by the applicant

- *Types of Classes: Depending upon requirement of assurance level and usage of DSC as described below, the applicant may select one of the classes.*

    Verification Process:
    - *Class-1 Certificate:* HO has to ensure the validity of the details given in the DSC Request Form and verify the same.

    - *Class-2 Certificate:* HO has to ensure the validity of the details given in the DSC Request Form and authenticate the same. HO has to further send it to SIO/NIC-Coordinator for forwarding to NICCA. HO has to utilize various procedures to obtain probative evidence in respect of identity of the applicants by way of seeking photograph and documentary evidence of one of the items under point no. 9 (Identification details) for individual certificate.
    For SSL server certificate the HO has to ensure attestation of URL for Web Servers by Domain Name Registering Agency, location of web server.
    - *Class-3 Certificate:* In addition to the verification process required for the class II certificates, the applicant's of class III certificates are required to be personally present with proof of their identity to the NIC-CA for issuance of DSC.

- On receipt of DSC application form, SIO/ DIO/HOD/NIC-Co-ordinator is required to ensure that the application form is signed by the HO(Head of Office)/JS/Company Secretary/Superior Officer of the applicant along with the seal of the office.

---oOo---