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:

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

Affix Recent Passport Size Photograph

Type of Applicant/Subscriber : **Government/ PSU & Statutory Bodies/ Registered Companies**

1. Class of Certificate Required **(see point 12 at page-4)** : **Class I** ☐ **Class II** ☐ **Class III** ☐
2. Certificate Required (Purpose) **(see point 12 at page-4)** : **Individual (Signing)**/Encryption/SSL Server (Web Server)/ SSL Client/ Time Stamping/ OCSP Responder/ OCSP Signer/ Smart Card Login/ Code Signing/ Time Stamping/ IP Sec Tunnel/ IP Sec User/ Key Recovery
3. Certificate Validity (**Max. 2 Years**) : One year/**Two year**/Specify validity_____
4. Name* : _____ (First Name) (Middle Name) (Surname)
5. Designation (Optional) : _____
6. Email Address(Official E-mail ID preferred) : _____
7. a) Office Address : _____
   Ministry/Department (Optional) _____
   _____
   _____
   Telephone:_____ (Official) _____(Residential)
   b) Residential Address : _____
   _____
8. Identification Details **(One or more)** : Employee Id/Code No._____
   Passport No. _____
   PAN Card No _____
   Voter's ID Card No. _____
   Driving License No. _____
   PF No. _____
   Bank Account Details _____
   Ration Card No. _____
9. In case the application is for a device then details of Server/Device for which the certificate is being applied for must be filled. (Details for **Server Certificate**) : Web Server _____
   Services _____
   IP Address _____
   URL/Domain Name _____
   Physical Location _____
10. The following details will be used in Certificate subject: : Organization* _____
    Organization Unit* _____
    Locality/City* _____
    State* _____
    Country* INDIA

Date: ……..
Place:……..

……
(Signature of the Applicant)

(For NICCA Office use only)

SmartCard/USB Token Sr. No.: **……..….**

Request No.:……..
RA code :……

Authorised Signatory / RAA: (**)**

(Name) **: (…….)**

Date:……. 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 understand that my organization name will be part of my DSC.
5. 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.**
6. I shall not use the private key before acceptance of the DSC.
7. I authorize NIC-CA to publish the certificate in the NIC-CA repository after acceptance of the DSC.
8. If the private key 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 NICCA-FRM-50037.Pdf, available under Repository>CPS & Forms>All Forms at https://nicca.nic.in)**
9. No attempt will be made to gain unauthorized access to NIC-CA facilities.
10. 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.
11. I understand that on cessation of my employment, I shall inform NICCA and my present employer for revocation of my Digital Signature Certificate.
12. I certify the following: *(Tick whichever is applicable)*
    - I have not applied for a DSC with NIC-CA earlier. ☐
    - I have been issued a DSC by NIC-CA with Serial no. _____ and Class- .The status of this DSC is Valid/Revoked/Suspended/Expired. ☐

The information furnished above is true to the best of my knowledge and belief. I will comply with terms and conditions of the Duties of Subscriber (as in section 40-42 of the IT Act2000) 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.

Place: …… (**Signature of the Applicant**)
Date: ……. Name: ……..…….

For Head of Office or JS (Admn.) for Government Sector/Superior Authority for Banking Sector of Applicant/ Company Secretary of Govt. registered Company

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 Digital Certificate from NIC-CA for the purpose specified above.

Date: ……..
Place: …….
Name of Officer with Designation:

(Signature of Officer with stamp of Org./Office)

Office Email: …….

Verification by SIO / HOD of NIC
(*Only for **Class-2** & **Class-3** Certificate*)

(Signature of HOD/SIO, NIC)
Name: ……..
Date: ……...
Office Seal:

This form has to be forwarded to NIC-CA at the following address:

National Informatics Centre Certifying Authority (NICCA)
National Informatics Centre
1st Floor, A-Block,
CGO Complex, Lodi Road,
New Delhi - 110003,
Telephone : 24366176

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.

I certify the following: *(Tick whichever is applicable)*

- I have not applied for a Encryption Certificate with NIC-CA earlier. ☐
- I have been issued a Encryption Certificate by NIC-CA with Serial no. _____ and Class …….The status of this Encryption Certificate is Valid/Revoked/Suspended/Expired. ☐

The information furnished above is true to the best of my knowledge and belief. I will comply with terms and conditions of the Duties of Subscriber (as in section 40-42 of the IT Act2000) 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.

Place: …… (**Signature of the Applicant**)
Date: ……. Name: ……..…….

Declaration by For Head of Office or JS (Admn.)

I hereby authorize Mr/Mrs…… 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 for Encryption key pair, 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: ……..
Name & Designation:
……. (Signature of Officer with stamp of Org./Office)
Office Email: ……..

Verification by SIO / HOD of NIC

(Signature of HOD/SIO, NIC)
Name: ……..
Date: ……..
Office Seal :

This form has to be forwarded to NIC-CA at the following address:

National Informatics Centre Certifying Authority (NICCA)
NIC, 1st Floor, A-Block,
CGO Complex, Lodi Road, New Delhi - 110003, Telephone : 011-24366176

Instruction for DSC Applicant

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/Netscape 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. The DSC form is required to be filled in duplicate which is downloadable under Repository>CPS & Forms> All Forms>NICCA-FRM-50034.pdf from https://nicca.nic.in. Photocopy of filled form in original signature will also be accepted. After filling the form, the applicant has to submit the application to his parent Department/Ministry for further processing.
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 pairs request and download certificate within 90 days) failing which; user is required to re-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 (Doc Id: NICCA-FRM-50037)
7. For viewing all valid DSCs and CRLs, the user can access the website (https://nicca.nic.in/) under Repository.
8. DSCs are issued on FIPS-140 Level-2 compliant smart card, which allows only maximum **ten numbers of incorrect attempts** for entering pass phrase/ pin. On exceeding this limit, the smart card gets blocked which can't be unblocked even by NIC-CA and hence DSC will have to be revoked and reissued.
9. It is important to note that email-id given by the applicant is functional and applicant access the same on regular basis as all communications in regard to DSC like user, revocation, renewal, expiration details is communicated thru the given email-id.
10. I understand that on cessation of my employment, I shall inform my present employer and NICCA for revocation of my Digital Signature Certificate.
11. For any further clarification, user can write to support@camail.nic.in or visit the NIC-CA website (https://nicca.nic.in).

12. ***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 and also encryption certificate may also be used for encryption requirement as per his/her official capacity.

Category Issued to Government entities/Head of the Institutions, Statutory/Autonomous bodies, Government registered Companies

Guidelines for verification for Head of Office or JS (Admn.) for Government Sector/Superior Authority for Banking Sector of Applicant/ Company Secretary of Govt. registered Company/ SIO/ DIO/HOD/NIC-Co-ordinator of NIC

- 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 maintain complete record of documentary proofs, one copy of dully-filled DSC form by the applicant and verified by them, in their offices. The **2nd** copy of application, they have to send to **NICCA [for Class I]** or SIO/ DIO/HOD/NIC-Co-ordinator NIC [**for Class II and III**].
- They have to ensure verification process as described below, depending upon the class of certificate as applied by the applicant

  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 ensures for the certainty of the details given in the DSC Request Form and authenticates the details, which is further authenticated by HOD/SIO/DIO/NIC-Coordinator. 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 8** (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 subscriber'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.
- SIO/ DIO/HOD/NIC-Co-ordinator has to maintain information for the applicants (Class-II or Class-III Certificates only) being authenticated by them by keeping photocopy of documentary proofs, DSC forms etc. They have to forward original copy of DSC form to NICCA for further processing.
- HO/ SIO/ DIO/HOD/NIC-Co-ordinator are requested to check class of certificates as per the instructions at point 12 on Page-4 of '**Instruction for DSC Applicant'.**