

**Government of West Bengal
Finance Department
Audit Branch**

No. 3739-F(Y).

Kolkata, the 3rd May, 2012.

NOTIFICATION

Sub: Mandatory publication of 'Tender Inviting Notice' on e-Tender Portal

For some time past the Government was considering improving the present system of inviting Tender by different Departments of the State Government with a view to establish accountability, transparency and uniformity in the system in a centralised manner.

Keeping in view the above object, the National Informatics Centre [NIC], an organisation of Government of India, developed a portal [<http://wbtenders.gov.in>] exclusively for uploading the tender related documents of the State Government.

The 'e-Procurement Solution' will help both the Government buyers and the suppliers to reduce the cycle time, unnecessary paper work, waiting in long queues and simultaneously enhance the transparency in the entire process thereby ensuring good governance. It is an easy-to-use, web-based solution for conducting dynamic exchanges in an on-line environment. It will provide real-time bidding solutions for the Government buyers and sellers. Some State Government Departments are already using this portal for inviting their e-Tender.

For the purpose of gainful utilisation of the said portal, the Governor has been pleased to decide that:

1. In addition to existing system of inviting tender, it will be mandatory for all State Government Departments, their subordinate Offices and all Autonomous Bodies / Local Bodies / Corporations / PSUs under their control to publish their 'Tender Related Information' [TRI] on the centralized e-Tender Portal [<http://wbtenders.gov.in>] if the Tender Value is Rs.50 lakhs and above. The Tender Value less than Rs.50 lakhs may also be uploaded on the centralized e-Tender Portal [<http://wbtenders.gov.in>] at the discretion of the Tender floating authority or the concerned Department.
2. The 'Tender Related Information' means and covers e-Procurement, e-Tendering, e-Selling and e-Auction, Request for Proposal, Request for Expression of Interest, Notice for Pre-Qualification, Registration of the Contractors, Notice inviting Tender/Bid or Proposal in any form, Tender Enquiries, Corrigenda and also the details of the contract awarded as a result of finalization of the Tender process.
3. The Departments or its subordinate offices that are already publishing their 'Tender Related Information' on their own websites and/or on any other websites shall ensure that their 'Tender Related Information' are simultaneously published / mirrored on the centralized e-Tender Portal [<http://wbtenders.gov.in>].
4. The Digital Signature Certificate, which is essential, for e-Tendering shall be obtained from the NIC-CA which is also acting as a Certifying Authority.
5. This Order shall take effect from 1st July 2012.

In order to facilitate implementation of aforesaid decisions regarding e-Publication of 'Tender Related Information' on the centralized e-Tender Portal, the

NIC will provide detailed guidelines for using the said Portal. The guidelines will also be available on the centralized e-Tender Portal [<http://wbenders.gov.in>]. On registration by the Government user, 'User ID' and 'Password' will be created and mailed to the users. The Government of West Bengal will also make arrangements for necessary training to the concerned officials, with technical support from NIC for the users of the e-Tendering Portal.

A Roadmap for implementation of the e-Procurement Process in the Government Departments is enclosed with this Order.

The Departmental heads are requested to circulate this Notification to their subordinate Offices and the Autonomous Bodies / Local Bodies / Corporations / PSUs under their control.

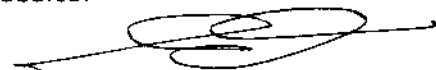
Sd/- H.K. Dwivedi.
Secretary to the
Government of West Bengal.

No. 3739/1 (150) -F(Y).

Kolkata, the 3rd May, 2012.

Copy forwarded for information and necessary action to :-

1. The Principal Accountant General (A&E), West Bengal, Treasury Buildings, 2, Govt. Place (West), Kolkata-700 001.
2. The Principal Accountant General (Audit), West Bengal, Treasury Buildings, 2, Govt. Place (West), Kolkata-700 001.
3. The Accountant General (R.W. & L.B. Audit), West Bengal, C.G.O. Complex, 'C' East Wing, 5th Floor, Salt Lake, Sector-I, Kolkata-700 064.
4. The Additional Chief Secretary/Principal Secretary/Secretary ,
.....Department.
5. The State Information Officer, National Informatics Centre, Bidyut Bhaban, Ground Floor, D.J. Block, Sector-II, Salt Lake, Kolkata-700 091.
6. The Director of Treasuries & Accounts, West Bengal, The New India Assurance Building, 4, Lyons Range, Kolkata - 700 001.
7. The Pay & Accounts Officer, Kolkata Pay & Accounts Office - I, 81/2/2, Phears Lane, Kolkata - 700 012.
8. The Pay & Accounts Officer, Kolkata Pay & Accounts Office - II, P-1, Hyde Lane, Kolkata - 700 012.
9. The Treasury Officer, _____.
10. Sr. P.A. to the Chief Secretary, Government of West Bengal.
11. Sr. P.A. to the Secretary, Finance Department, Govt. of West Bengal.
12. _____
13. Sri Sukumar Negel, Pr. Accounts Officer & Ex-Officio Deputy Secretary, Finance (Budget) Department, Writers Buildings, Kolkata-700001, for uploading the Notification in the Finance Department's website.



(Swapan Kumar Paul)
Special Secretary to the
Government of West Bengal.
Finance Department.

Roadmap for implementation of e-Procurement Process in the Government Departments

1. Each Department shall nominate at least one 'Nodal Officer' for implementation and monitoring of the **e-Procurement** in the respective department.
2. The Nodal Officer of the Department shall handover to NIC the organisation chart related to tendering in his Department mentioning the offices from where tenders will be floated or published in the Portal.
3. Nodal Officer shall apply to NIC for Digital Signature Certificate [DSC] as Nodal Officer on behalf of that Department for implementing e-Procurement.
4. The other Departmental Officers who will be authorised to float e-Tender under a Department shall be required to obtain DSC from NIC through the Nodal Officer of that Department. The cost of obtaining DSC from NIC is Rs.555/- per user. Application Form for Digital Signature Certificate [DSC] along with detailed information regarding Digital Signature Certificate is enclosed with this Roadmap.
5. For uploading the e-Tender document in the Tender Portal it will be required to have minimum two (2) authorised officers who have their own DSC. The DSC is neither transferable nor it can be delegated to other officer.
6. The DSC issued is Department specific and officer specific. So, it will not be possible for the authorised Officers (having DSC) of one Department to upload e-Tender of other Department.
7. In the headquarter, each Department shall nominate at least two officers who will be members of each Tender Committee under that Department, so that they can upload the e-Tender document in the Tender Portal on the authorisation of their DSC.
8. Similarly, in each District or Region (as per requirement of the Department) the Department shall nominate at least two officers who will be members of each Tender Committee on behalf of that Department, so that they can upload the e-Tender document in the Tender Portal on the authorisation of their DSC.
9. Summary information in respect of the Tender progress in relation to the Tender has to be uploaded in the web-server of the Tender Portal. Documents relating to 'Notice Inviting Tender' [NIT] shall be loaded as a .pdf file and the financial bid in the prescribed .xls format. For the financial bid NIC has developed three templates that have to be strictly adhered to. The Tendering Authority shall select any one of the three formats which will be suitable for them for that particular Tender. The software developed by NIC shall take care for selection of L1 rates. The Software shall make automatic encryption of the Financial Bid and no one shall be allowed to open the Financial Bid prior to the date & time earmarked for opening the Financial Bid. Tender should normally be floated in two parts, one Technical bid and other Financial Bid. After evaluation of the Technical Bid, those who qualify their Financial Bid shall be opened.

10. (i) NIC at headquarter or at any central location, preferably within Writers Buildings, shall provide a "Helpdesk" to render necessary help to the authorised officers of the Departments within Kolkata (including Bidhannagar) to float e-Tender.
- (ii) The District Information Officers [DIO] of NIC at the District shall provide a "Helpdesk" to render necessary help to the authorised officers of the Departments at the District level.

Necessary information regarding Digital Signature Certificate [DSC]

1. What is a Digital Signature Certificate?

Digital Signature Certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as a proof of identity of an individual for a certain purpose; for example, a driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally.

2. Why is Digital Signature Certificate (DSC) required?

Like physical documents are signed manually, electronic documents, for example e-forms are required to be signed digitally using a Digital Signature Certificate. Transactions that are done using Internet if signed using a Digital Signature certificate becomes legally valid.

3. Who issues the Digital Signature Certificate?

A licensed Certifying Authority (CA) issues the digital signature. Certifying Authority (CA) means a person who has been granted a license to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000. The National Informatics Centre is also authorised to issue the Digital Signature Certificate.

4. What are the different types of Digital Signature Certificates valid for e-Tendering programme ?

The different types of Digital Signature Certificates are:

Class 2: Here, the identity of a person is verified against a trusted, pre-verified database.

Class 3: This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/ her identity.

5. What type of Digital Signature Certificate (DSC) is to be obtained for e-Filing on the e-Tendering Portal?

DSC of Class 2 and Class 3 category issued by a licensed Certifying Authority (CA) needs to be obtained for e-filing on the e-Tendering Portal.

6. How to obtain DSC for dept users?

NIC hqrs is authorised to issue the DSC for officials in Govt depts./PSUs and the fees are:

For Govt Officials Rs. 555 for USB e-Token (at present)

The validity period for the Smart Card is 2 years.

The DD should be drawn in favour of "Accounts Officer, National Informatics Centre, New Delhi".

7. How much time do CAs take to issue a DSC?

The time taken by Certifying Authorities to issue a DSC may vary from three to seven days.

8. What is the validity period of a Digital Signature Certificate?

The Certifying Authorities are authorized to issue a Digital Signature Certificate with a validity of one or two years. The maximum period for which the DSC is issued is only two years. On the expiry of the term, the Digital Signature Certificate can be revalidated by paying the fees again.

9. What is the legal status of a Digital Signature?

Digital Signatures are legally admissible in a Court of Law, as provided under the provisions of IT.

10. Is a company required to obtain a Digital Signature Certificate in its own name for e-Tendering.

Digital Signature Certificate (DSC) is not required by Companies but by individuals. For example the Director or the Authorized signatory signing on behalf of the Company requires a DSC.

11. Can I do e-filing of documents if I do not possess a DSC?

No. It is mandatory to have a valid digital signature certificate for e-filing the forms on e-Tendering portal.

**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. 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.



<p>1. Category of Applicant</p> <p>2. Class of Certificate Required (see pt. 11 at page 4)</p> <p>3. Certificate Required (Usage) (see pt. 11 at page 4)</p> <p>4. Certificate Validity (Max. 2 Years)</p> <p>5. Date of superannuation* (dd/mm/yyyy)</p> <p>6. Name*</p> <p>7. Designation</p> <p>8. Email ID* (Official email-ID preferred)</p> <p>9. Ministry/Department</p> <p style="margin-left: 20px;">a) Office Address</p> <p style="margin-left: 20px;">b) Residential Address</p> <p>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.]</p> <p>11. Certificate Subject Details* (These will be used in Certificate subject)</p> <p>12. SSL Certificate Details (In case the application is for a device then details of Server/Device for which the certificate is being applied for must be filled.)</p>	<p>Government / Judiciary / PSU & Statutory Bodies / Registered Companies</p> <p>Class I / Class II / Class III</p> <p>Individual (Signing) / Encryption / SSL Server</p> <p>Two years / Specify validity (if less than 2 years) _____</p> <p>_____</p> <p>_____</p> <p align="center">(First Name) (Middle Name) (Last Name)</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>Telephone (Official) _____ (Resi/Mobile) _____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>Organization* _____</p> <p>Organization Unit* _____</p> <p>City* _____</p> <p>State* _____</p> <p>Country* INDIA</p> <p>Web Server _____</p> <p>Services _____</p> <p>IP Address _____</p> <p>URL/Domain Name _____</p> <p>Physical Location _____</p>
---	---

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 employment.

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)*
 - o I have not applied for an Encryption Certificate with NIC-CA earlier.
 - o 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--