

No.1/90/2012-1SII
HARYANA GOVERNMENT
CHIEF SECRETARY'S OFFICE
PERSONNEL DEPARTMENT

Chandigarh :Dated 17th August, 2012

To

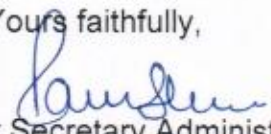
The All Deputy Commissioners,
in the State.

Subject:- Issuance of Digital Signature to the officers having the charge of ERO/
AERO.

Sir/Madam,

I am directed to refer to the subject noted above and to enclose a copy of letter dated 04.11.2010 and 17.02.2011 alongwith guidelines issued by Election Commission of India with the request to get the filled in Digital Signature Certificate Request Form from all the DEOs and ERO/AEROs and as such other officers working as Tehsildar, District Development & Panchayat Officer and Block Development & Panchayat Officer etc. working in their districts and to send the same to SIO, NIC, Haryana Civil Secretariat, Chandigarh at the earliest for its onward transmission to NIC, New Delhi so that digital signature could be issued in their favour. It is also requested that whenever an officer working as ERO/AERO and such other officer working as Tehsildar, District Development & Panchayat Officer and Block Development & Panchayat Officer etc. is transferred a fresh process may be started to get the digital signature issued in his/her favour.

Yours faithfully,

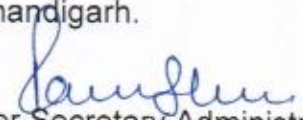

Under Secretary Administration,
for Chief Secretary to Government, Haryana

Endst.No.1/90/2012-1SII

Dated:Chandigarh, the 17.08.2012

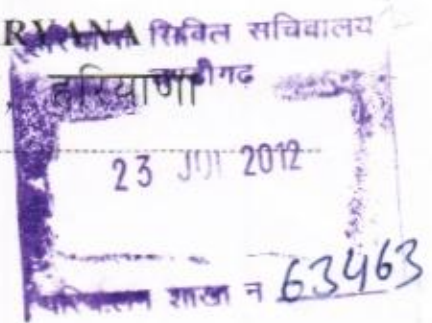
A copy, alongwith copies of letters dated 04.11.2010 and 17.02.2011 of Election Commission of India is forwarded for information and necessary action to :-

- 1.The Additional Chief Secretary to Govt., Haryana and Financial Commissioner, Revenue & Disaster Management and Consolidation Departments.
- 2.The Principal Secretary to Govt., Haryana, Development & Panchayats Department.
- 3.The SIO, NIC, Haryana Civil Secretariat, Chandigarh.


Under Secretary Administration,
for Chief Secretary to Government, Haryana



OFFICE OF
CHIEF ELECTORAL OFFICER, HARYANA
कार्यालय मुख्य निर्वाचन अधिकारी, हरियाणा



The Chief Secretary,
Govt. of Haryana.

Elect/2012/AE-V- 3965

Dated:- 18-7-2012

CS/om/tauf
24/7/12
PS/LS

Subject: Issuance of Digital Signature to the officer having which the charge of ERO/AERO.

Sir,

On the subject noted above I am directed to state that Election Commission of India vide its letter bearing No. 485/Comp/ERMS/2010, Dated 4.11.2010 and No. 485/Comp/DC/2010, Dated 17.2.2011 has issued directions to issue the Digital Signatures to the officers having the charge of ERO/AERO.

A copy of the Commission letter along with guideline is attached herewith.

In this regard it is further submitted that ERO/AERO are appointed amongst the cadre of IAS/HCS & such officers working as Tehsildar, DDPO, BDPO etc.

In compliance of Commission direction all ERO/AERO should have digital signatures. Whenever officer is transferred afresh process has to be started to get the digital signature issued in their favor. Whereas work of Electoral revision is time bound and needs to be completed within the specified schedule as is fixed by the Election Commission of India. In such a situation the Revision process has to face difficulties in processing the digital signature in favor of new officer within a short span of time.

In view of the situation, it is requested that Digital Signatures may be issued to all officers of IAS, HCS being posted as ERO/AEROs and other officers like Tehsildar DDPOs and BDPO so that the process of Electoral Revision does not suffer due to technical issues like Digital Signature.



Your's Faithfully,

Deputy Chief Electoral Officer,
for Chief Electoral Officer, Haryana.

ELECTION COMMISSION OF INDIA

Nirvachan Sadan, Ashoka Road, New Delhi-110 001.

No.485/Comp/ERMS/2010

Dated : 4.11.2010.



The Chief Electoral Officers of
All States and Union Territories (except Bihar)

Subject:

Deployment of ERMS – Issuance of Digital Signature Cards – regarding.

Sir/Madam,

Use of digital signature authorization has been added in the ERO module of ERMS developed by ECI. New version of ERMS can be downloaded from :-

- FTP Address: 164.100.34.8
- Folder Name: ERMS & Admin Module Software 4 Nov 2010

In order to use digital signature authentication, Digital Signature Cards need to be procured from NIC or other GOI credited agencies by the CEOs. These cards should be sent by special messenger to DEOs. The DEOs shall distribute these cards to EROs/AEROs.

It may be noted that digital signature cards (DSCs) should not repeat **NOT** be sent by post or Courier. It should be ensured that they are sent through special messenger and should be handed over to the DEOs in person under proper acknowledgement. The DEOs in turn should call the EROs/AEROs to their offices and hand over the DSCs to them in person again under proper acknowledgement.

The procedure to obtain the DSCs from NIC is given below -

1. Fill up form for digital signature certificate card and card reader.
2. Obtain digital signature card and card reader.
3. Open <http://nicca.nic.in/>
4. Click Support Menu
5. Download Driver S/W:SC Reader,USB/iKey Token

6. Click StarKey/G&D SafeSign identity-client Download [.zip format]
(for all Windows XP/Vista/7 - 32/64 bit OS)
7. Find a folder with name eTokenG&D-starkey (downloaded)
8. Open this folder
9. For 32-bit system, open folder with name '32' and install both the drivers
10. After completing installation :
11. Open Program - > SafeSign Standard - > Token Administration
12. Select your name from the given window and then right click to select option Initialize
Token option
13. Fill up all the details such as default PUK is '0000' and default PIN is '1234'
14. Now check your Token Status, it would be operational now.
15. Now again, Open <http://nicca.nic.in/>
16. Click 'Member Login' option
17. Enter your user id and password mentioned on your digital card (Right bottom). The
default user id and password is same.
18. After successfully login, select Step 1 : Enroll for Digital Certificate
19. Read the instruction carefully
20. Fill up your Enrollment Form and select Certificate Type is 'Signing Certificate' and
Cryptography Service Provider is SafeSign Standard Cryptographic Service Provider
21. Click on Generate Request button
22. Request No may be used to track the current status of your application
23. Collect your PIN from your email account provided by the agency
24. Now again, Open <http://nicca.nic.in/>
25. Select option - > Step 4 : Download your Digital Signature
26. From the given list, click your Request No (Hyperlink)

27. Verify your profile details and enter authentication PIN provided in your mail and click on 'Download' button. (Please note that you must keep your digital card in the card reader to download the certificate)
28. Now, after successfully downloading the certificate.
29. Open Program -> SafeSign Standard -> Token Administration
30. Select your account and right click to choose show token object
31. Now you can view your digital certificate.

Before distributing the cards to EROs / AEROs & DEOs, the digital certificate should be saved in the database. Unless this is done, the DSC will not be usable by the user. This can be done in the following manner through the Admin module :-

1. Open and execute Admin module
2. Enter User Id is Admin and Password is aDmin (Default Settings)
3. Select Summary Revision ERO Menu Item
4. Create New User and allot AC and Parts
5. Now, feed digital card information and make sure the card is in card reader.
6. Select a user and click on Save Digital Card Information.

Kindly acknowledge receipt.

Yours faithfully,

(J.K.RAO)
UNDER SECRETARY

D.No - 372
4-3-2011

-3-

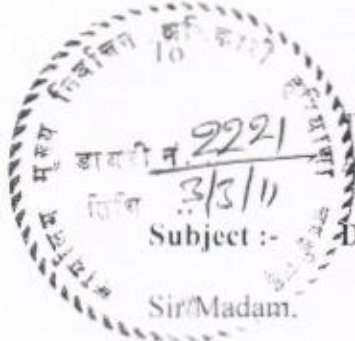
CEO
Date 28-2-11
Add CEO
USE

ELECTION COMMISSION OF INDIA

Nirvachan Sadan, Ashoka Road, New Delhi-110 001.

No 485/Comp/DC/2010

Dated : 17.02.2011.



The Chief Electoral Officers of
all States and Union Territories.

Subject :- Deployment of ERMS - Issuance of Digital Signature Cards - regarding.

The Commission intends to issue the Digital Signature Cards to all the District Election Officers of all the States / UTs for various applications of the Commission. In this regard, I am directed to enclose herewith the blank 'Digital Signature Certificate Request Form' and request you to forward the same to all the DEOs of your State and get the filled in Digital Signature Certificate Request Form from all the DEOs and submit the same through SIOs, alongwith the consolidated fees @ Rs.716/- per Digital Signature Card in the form of Demand Draft in favour of Accounts Officer / DDO (as per the list attached), to the respective NIC Certifying Authority RA Office of the respective State. For the States / UTs which are not in the list, the Demand Draft should be in favour of Accounts Officer / DDO of the adjoining State / UT.

Yours faithfully,

(J.K. RAO)

UNDER SECRETARY

-10-

**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.

Affix Recent
Passport Size
Photograph

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 _____
5 Name*	_____ (First Name) (Middle Name) (Last Name)
6 Designation	_____
7 Email ID* (Official email-ID preferred)	_____
8 Ministry/Department	_____
a) Office Address	_____ _____ _____
	Telephone (Official) _____ (Resi/Mobile) _____
b) Residential Address	_____ _____ _____
9 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.]	_____ _____ _____
10 Certificate Subject Details* (These will be used in Certificate subject.)	Organization* _____ Organization Unit* _____ City* _____ State* _____ Country* INDIA
11 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.)	Web Server _____ Services _____ IP Address _____ 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)*
 - ☐ I have not applied for a DSC with NIC-CA earlier.
 - ☐ 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 by Head of Office of Applicant

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 Certificate from NIC-CA for the purpose specified above.

Date : _____ (Signature of Officer with stamp of Org./Office)
Place : _____ 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.

-12-

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---

15

Certificate Fee Structure (in ₹)
(for all classes: Class-I, Class-II & Class-III)

Type of Subscribers	Smart Card Individual personal Certificate				USB Token/iKey Individual personal Certificate			Soft Token SSI Server Device Cert. (Proc. charge)	Renewal (Proc.Charge)
	Smart Card	Proc. and Material	Proc. Charge	Total	USB Token	Proc. Charge	Total		
Individual	227/-	489/-	-	716/-	555/-	-	555/-	-	-
Government	227/-	489/-	200/-	916/-	555/-	200/-	755/-	200/-	200/-
Validity	Two years (Conditions apply)								
	On expiry of certificate, processing charge shall be applicable as above to renew/create the certificate on the same media. All other formalities shall be same as for a new DSC applicant, including submission of fresh DSC Application form and fees as applicable.								
For more detailed information on device drivers, etc., please refer to SCM website: http://www.scmicro.com									
Mode of Payment (Demand Draft/RBI Cheque)									
DSC form submitted to NICCA RA Office, Delhi/Chandigarh/Hyderabad: DD in favour of "Accounts Officer, NIC Delhi" payable at New Delhi									
DSC form submitted to NICCA RA Office, Lucknow: DD in favour of "DDO, NIC UP State Centre" payable at Lucknow									
DSC form submitted to NICCA RA Office, Bangalore: DD in favour of "DDO, NIC Karnataka State Centre" payable at Bangalore									
DSC form submitted to NICCA RA Office, Chennai: DD in favour of "DDO, NIC Tamilnadu State Centre" payable at Chennai									
DSC form submitted to NICCA RA Office, Bhubaneswar: DD in favour of "DDO, NIC Bhubaneswar" payable at Bhubaneswar									
DSC form submitted to NICCA RA Office, Guwahati: DD in favour of "DDO, NIC Assam State Centre" payable at Guwahati									
DSC form submitted to NICCA RA Office, Raipur: DD in favour of "DDO, NIC Chhattisgarh State Centre" payable at Raipur									

[Click here to Download DSC request Application Form](#)

[Download SmartCard driver & Token](#)