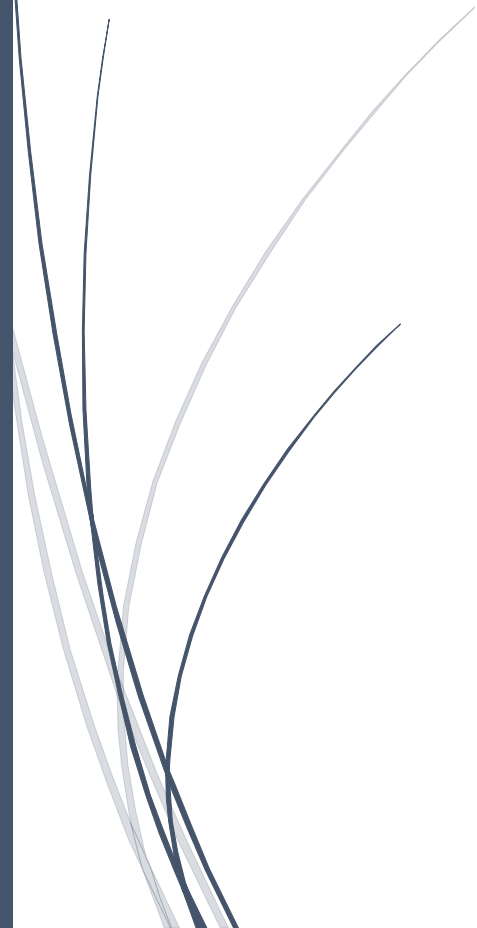6/1/2020

Prerequisite Guidance Document on DSC Roll out

Background of the Program:

- There are nine target supported states by the World Bank under its Program Towards Elimination of Tuberculosis (PTET) and as per DLI 2.1, targeted states must initiate DBT payments using Digital Signature Certificate (DSC)

- For Year 1 ('19 – '20) of DLI State's target is to achieve coverage in 20% districts with an increase of 20% every subsequent year till Year 4

- A directive guideline was issued by CTD[1] in the month of January '20 and received at State

- This guidance documents aims to ease the DSC Implementation process by highlighting steps which States may adopt to achieve rollout of the DSCs under the Program

Brief Overview of Digital Signatures

Before States take up the Implementation and rollout of DSCs it is important to also understand what Digital Signatures are and what is the difference between Digital Signatures and Handwritten Signatures.

1. **Digital Signatures -**

    A digital signature is an electronic signature that can be used to authenticate the identity of the signer of a document. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time stamped. A digital signature can be used with any kind of message, whether it is encrypted or plaintext. Thus, Digital Signatures provide the following three features[2]: -

    a) Authentication - Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user

    b) Integrity - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions

    c) Non-Repudiation – Digital signatures ensure that the sender who has signed the information cannot later deny having signed it

2. **Digital Signatures versus Handwritten Signatures**

    A handwritten signature scanned and digitally attached with a document does not qualify as a Digital Signature. An ink signature can be easily replicated from one document to another by copying the image manually or electronically. Digital Signatures cryptographically (*protecting information by transforming it in secure format*) bind an electronic identity to an electronic document and the digital signature cannot be copied to another document.

---

[1] Central Tuberculosis Division
[2] Ministry of Communications and Information Technology, Government of India

A. Pre-Implementation Process

Below section details the process of three major activities which should ideally be carried out before the actual Implementation starts at pre identified sites.

I. Formation of Core Committee

It is advised to States to form the Core committee to implement the program smoothly. Following members could be part of this Committee-

At State Level

1. Director- Public and Health Services (PHS) / Finance-NHM[3]
2. State Accounts officers + one member from IT Department
3. PFMS[4] Consultant
4. Program Partner person who will be managing the entire program

At District Level

1. CMHO[5]/ACMO
     i. District Accounts Manager
     ii. Data entry operator to support
2. District TB-Officers
     i. District Accounts Officer
     ii. Data entry operator to support

II. Administrative Process: (at State Level)

After receipt of email from CTD following three steps should ideally by followed at State Program Office to ensure timely procurement of DSCs. (*Please refer Annexure-1 for email from CTD*).

1. STO to initiate file for seeking necessary approvals from the authorities (Director-Finance, MD-NHM, and PS[6] / ACS -Health) on rollout of DSC-System for all the DBT-Payments as per the State General Financial Rules under the program

2. STO to nominate one person (State Account Officer or as decided) under which the DSC Implementation will take place

3. It is also advised that a directive communication may be given by the office of Director-PHS to all the CMHO's and DTO's, highlighting that under the NTEP[7] the DBT payments in following schemes (*as highlighted below*) must be routed through Digital Signature Certificates only. The District Program Committee (TB) which ideally comprises of Member Secretary (DTO) and the Chairman (CMHO) should confirm back to the State Program Office on the procurement of the DSC keys within seven days.

---

[3] National Health Mission
[4] Public Financial Management System
[5] Chief Medical Health Officer
[6] Principal Secretary
[7] National Tuberculosis Elimination Program

      i.   Nikshay Poshan Yojana
      ii.   Private Provider Incentive Scheme
      iii.   Tribal support Scheme
      iv.   Treatment supporter Honorarium

III.   Procurement Process of Digital Signature Certificate (DSC)

The procurement of DSC can be undertaken from any authorized agency by NIC[8] (*Refer to Annexure -2 as list of Certified authorities and Annexure- 3 for the Sample request form*)

With reference to point no 3, It was also advised that the District authorities (DTO/CHMO) might book the expenditure for DSC-Procurement under **"Office Operation"** head. In cases where there is no budget available, the DPC should reach out to the State TB Office.

B.   Other prerequisite requirements for Implementation
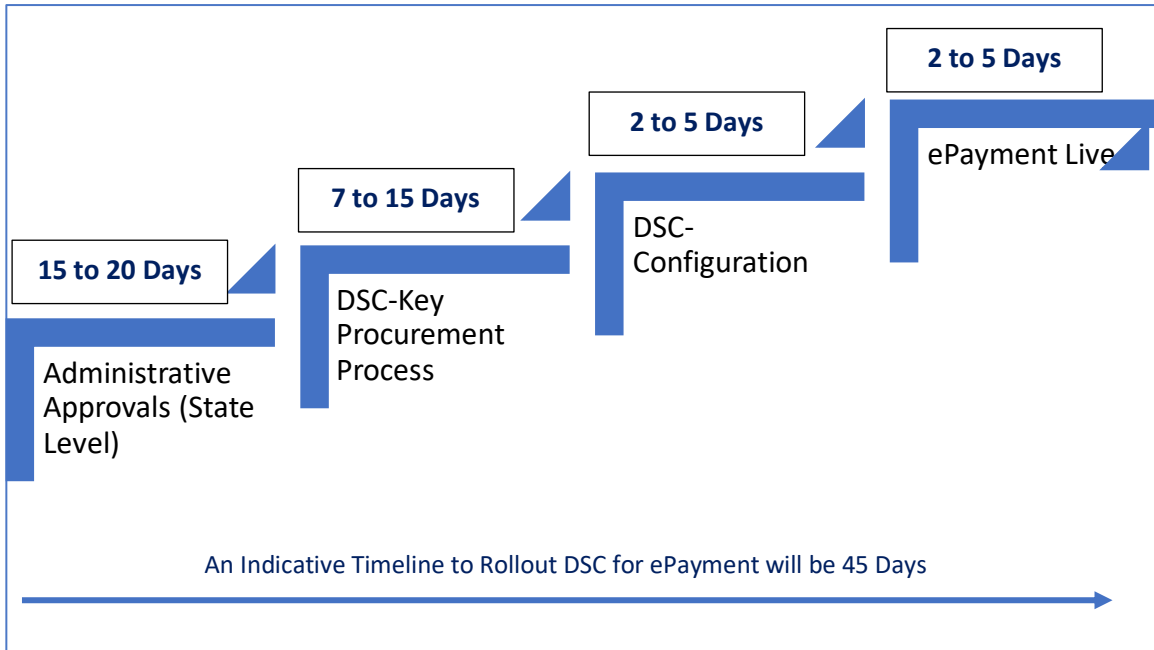
Hardware Prerequisite:

1. The Computer machine / Desktop which is used for the DSC setup should support the PFMS-system settings

System Software Prerequisites:

1. Computer- Operating System
   a. Operating system for DSC-setup should at least be Windows 7
   b. In case of Windows 7 Operating system, Service Pack 1 must be installed in the system

2. Add-On Applications
   a. Internet Explorer 11 must be installed in the system

3. Application Software
   a. The latest JAVA-with its update must be installed in the system.
      i. Please refer to link https://www.java.com/en/download/
      ii. Or the installation guide available on the link https://nikshay.zendesk.com/hc/en-us/sections/360008223952-DSC-based-payments-in-PFMS.

   b. Installation of DSC-Key Drivers and applications.
      i. Installation of Driver for DSC-key is a onetime activity, and it automatically runs during the enrollment of DSC-Key in PFMS
      ii. Please refer to link https://nikshay.zendesk.com/hc/en-us/sections/360008223952-DSC-based-payments-in-PFMS and the slide number 16

---

[8] National Informatics Centre

In the end, the below exhibit also shares the approximate timelines for DSC Implementation Go-Live

2 to 5 Days	ePayment Live
2 to 5 Days	DSC-Configuration
7 to 15 Days	DSC-Key Procurement Process
15 to 20 Days	Administrative Approvals (State Level)

An Indicative Timeline to Rollout DSC for ePayment will be 45 Days

Note: This document is based on the learning experience during the DSC-Implementation in Rajasthan, there might be some procedural changes experienced during its implementation in other states as per the State General Financial Rules (GFR) and the best practices adopted by the state.

Annexure -1 (email from CTD)

On Mon, 27 Jan 2020 at 17:00, Dr Sudarsan Mandal <mandals@rntcp.org> wrote:

Dear STOs,

As you are aware that World Bank's Program Towards Elimination of Tuberculosis (PTET) for India is supporting following nine States for elimination of TB.

#	World Bank Targeted States
1)	Assam
2)	Bihar
3)	Karnataka
4)	Madhya Pradesh
5)	Maharashtra
6)	Rajasthan
7)	Tamil Nadu
8)	Uttar Pradesh
9)	West Bengal

As a part Disbursement Linked Indicators (DLI), The World Bank supported states have to make DBT payments by using **Digital Signature Certificate (DSC)**.

You are requested to initiate the process for getting Digital Signature Certificate (DSC), for all STOs and DTOs at the earliest. Necessary request form is attached which is self-explanatory. Kindly get in touch with respective NIC Units for the same.

DSC form can be downloaded from NIC website, which is https://vpn.nic.in/resources/application_forms/DSC-Request-Form.pdf.

Regards,

Dr Sudarsan Mandal
MD (SPM)
Addl.DDG (TB)
Central TB Division
Room No. 532 'C'-Wing,
Ministry of Health & Family Welfare
Nirman Bhawan, New Delhi-110011
Office Tel: (011) - 23061130
Email: mandals@rntcp.org

*Annexure -2 (*List of DSC-Key Certified agency from DSC-key can be purchased)

National Informatics Centre (NIC)	NIC
IDRBT Certifying Authority	IDRBT
SafeScrypt CA Services, Sify Communications Ltd.	SAFE SCRYPT
(n) Code Solutions CA	(n)Code Solutions e-Safe . e-Secure . e-Sure
E-MUDHRA	e mudhra Trust Delivered
CDAC	सी डैक CDAC
NSDL	NSDL Technology, Trust & Reach
Capricorn	Capricorn Identity Services Pvt. Ltd.

Or can be downloaded from below mentioned link.

http://www.mca.gov.in/MinistryV2/certifyingauthorities.html

Annexure -3 (Sample Request form)

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

Photo & ID proof to be attested by HO

Ref. No. ……………………………
(To be filled by NICCA/RA Office)

DIGITAL SIGNATURE CERTIFICATE REQUEST FORM

Affix Recent Passport size Photograph **Attested by HO**

NOTE:
1. READ INSTRUCTIONS FIRST. All fields are mandatory and validity of the filled form is 90 days.
2. Please Tick (**v**) the appropriate option & submit only Page No. 1 & 2 after filling.
3. Subscriber is advised to read Certificate Practice Statement of NICCA.
4. Validity period cannot exceed the date of superannuation of applicant.
5. Asterisk (*) mark entry will be used in Certificate Subject Details.
6. **INCOMPLETE/INCONSISTENT FORMS WILL BE SUMMARILY REJECTED.**

1. Category of Applicant   : _____ [*Fill code from Annexure-I*]

2. Project Code   : _____ [*Fill code from Annexure-II*]

3. Class of Certificate Required   : Class-1 /Class-2 /Class-3   Device Required: **No Device/Token/ Smart Card** only for **signing** certificate

4. Certificate Required (Usage)   : Signing /Encryption /SSL/System/Code Signing [**Separate Form for each except Signing/Encryption**]

5. Certificate Validity [Max. 2 Years]   : Two Years /Specify Validity [if less than 2 Years] _____

6. Date of Superannuation [DD/MM/YYYY]   : _____

7. Name* (in **BLOCK** letters only)   : _____

8. Designation   : _____

9. Email-id*[Official email-id preferred]   : _____

10.   Ministry/Department
     a) Office Address   : _____
          _____

          Tel. No.(O)* _____ **Mobile No.*** _____

     b) Residential Address   : _____

11.   Identification Details   : _____
    [*Attach a photocopy of the same attested by HO*]   [**Departmental / Employment Photo ID No./ Service Verification Certificate with photograph on official letter head**]

12.   Certificate Subject Details*   : Organisation* _____
          Organisation Unit* _____
          City* _____ Postal Code* _____
          State* _____ Country*   **INDIA**

    Only for PAN enabled DSC*   : **PAN No.*** _____ [Attach a self attested photo copy of PAN card, for **Company PAN enabled** DSC: provide a company PAN & documentary proof for holding position in the company]

13.   SSL/Web Server Certificate Details   : Public IP Address_____ Physical Location _____
    [*To be filled only for SSL certificate*]   URL/Domain Name _____
          Alternate Domain Name _____
          IP allocation Organisation_____

14.   System Certificate Details   : IP Address_____ MAC Address _____
    [**Any one detail required**]   Serial No./Unique Id (CPU/device)_____

15.   Payment Details   : DD No. _____ Date _____ Bank Name_____
          NICSI Project No., if any _____

Place: …………………..
Date: …………………..

       (Please do not write below this line)   [**Signature of Applicant**]
       (For NICCA/RA Office Use Only)

REF	SCAN	UID	SC/SCR	TKN	PRN

Req. No. (S)_____
Req. No. (E)_____

RAA Name ……………………… Date ……………...

[Version: DSC Form V 6.2 (Doc-Id. Form-1) Updated on: 25 June 2014]   Page 1

Ref. No.: ………………………………… *(To be filled by NICCA/RA Office)*

Physical Appearance Verification Details
(To be filled by NIC Verifying Officer for **Class-3** DSC applicant)

- ✓ In-person verification of Shri/Smt/Ms………………….…………….............Class-3 DSC applicant has been carried out on ………………… (dd/mm/yyyy) at ....(hh:mm).

- ✓ He/she has shown his/her departmental-id/Service verification letter bearing No. ……………………………………

- ✓ His/her signature & photograph have been matched with signature & photograph available on his/her departmental-id card/ Service verification letter as well as DSC application form.

- ✓ His/her signature & photograph have been attested by the undersigned as shown below.

- ✓ His/her mobile No. is …………..………………..

- ✓ Photocopy of departmental-id card attested by HO is attached herewith.

Paste passport size latest Photograph of Applicant (For class-3 certificate only) **Attested by NIC Verifying Officer**	**Applicant's Signature** (To be signed in the presence of verifying officer) ……………………………………………..

Photograph to be Attested by NIC Verifying Officer (Signature & Stamp across the photograph)

Attested/verified by:-

Name/Designation/Emp. Code
Email:
Telephone/Mob No.:
NIC Centre/Location:

[For Class-3 certificate only - This Annexure is to be attached with DSC form & forwarded to the respective NICCA/RA Office Please ensure all the fields are filled up]

[Version: DSC Form V 6.2 (Doc-Id. Form-1) Updated on: 25 June 2014]   Page 5

9. SSL Server certificates are not issued for <u>Private IPs</u>; it is issued only for <u>Public IPs</u>. The applicant has to fill the information about <u>IP address allocating Authority</u>.

10. **CERTIFICATE CLASSES, OID & ASSURANCE LEVEL**

Sr. No.	Class of Certificate	OID	Assurance Level/Verification Process
1.	Class-0	2.16.356.100.2.0	It carries no assurance, as it is created with general distinguished name not for an individual
2.	Class-1	2.16.356.100.2.1	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.
3.	Class-2	2.16.356.100.2.2	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.
4.	Class-3	2.16.356.100.2.3	Provides highest level of assurances, as verification process as in addition to the verification process required for the class-2 certificates, the applicants are required to be personally present at Physical Appearance Centre (PAC) for completion of in-person verification process.

11. The DSC applicant with category Govt/PSU/Judiciary/Statutory/Autonomous Bodies/Sector 25 Govt Company has to get his credentials verified from his/her **Head of the office of organisation,** contractual employee has to verify his credentials from his/her employer, the Elected Member (MP/MLA/Village Panchayat/Gram Sabha) has to verify his/her credentials from head secretariat/Panchayat.

12. For any further clarification, user can write to casupport@nic.in or visit the NIC-CA website (https://nicca.nic.in).

13. Issued certificates not downloaded within **2 weeks** shall be revoked without intimation to the applicant and a fresh form would be required for new certificate.

14. Media provided by NICCA is with a warranty of six months against manufacturing defects from the date of issuance. In case of manufacturing defect, the same shall be replaced, but for issuance of DSC, subscriber has to apply with a fresh form.

15. On loss/physical damage of USB Token/Smart Card, new media shall be issued after payment only. Also for issuance of new DSC, the subscriber has to revoke the previous issued (lost) DSC and submit a new form for DSC issuance.

16. The media provided by NICCA shall provide support for platforms as mentioned at NICCA website (https://nicca.nic.in) Also for platform which has become obsolete due to technology advancement, support shall be discontinued.

17. The applicant is responsible for preparation of his/her machine with all relevant software downloads from NICCA website or otherwise for certificate request creation and download from web interface of NICCA at (https://nicca.nic.in).

18. Authentication pin for downloading the certificate shall be sent ONLY to the email specified in the DSC request Form. Request for auth-pin from any other person will not be entertained. In case of accidental deletion/non-delivery of email containing the pin the DSC applicant has to send a mail from email id quoted in the application to casupport@nic.in for resending the authentication pin.

19. <u>Department photo-id card</u> has to be produced for completion of physical verification for Class-3 DSC applicant.

20. **Contractual employees** will be issued only **Class-1/Class-2 Signing** certificates.

21. NICCA IS NOT RESPONSIBLE FOR ANY POSTAL DELAYS OR LOSS OCCURING DURING THE TRANSIT OF THE MEDIA. NICCA CANNOT BE HELD LIABLE FOR THE SAME.

B. Guidelines for verification by Head of Office (HO)

The head of the office is appointed in the Govt. Department/Organisation. The Superior officer not necessarily be the Head of the Office (HO).

a. The **Head of Office (HO) of respective organizations/departments 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. **The onus of verification lies with Head of office (HO) of the Applicant.**

b. For the DSC applicant with category Govt/PSU/Judiciary/Statutory/Autonomous Bodies/Sector 25 Govt Company the credentials have to be verified by **Head of the office of organisation, for t**he contractual employee credentials have to be verified by his/her employer, for the Elected Member (MP/MLA/Village Panchayat/Gram Sabha) credentials have to be verified by secretary/ Panchayat Head.

c. The **HO of respective organizations/departments** must utilize various procedures to obtain evidence in respect of employment in Government Sector/contractual persons deployed for e-governance project by way of documentary evidence and cross examination of the same with available official records in their office.

d. For contractual employees, the HO has to get verified the credentials from the companies/vendors from where these contractual employees have been hired/outsourced by way of getting a letter on letter head from the company/vendor.

e. **Registration Authorities of NIC (NICRA) are not responsible for verification of credentials of the applicant.**

f. For SSL server certificate the **HO** has to ensure the correctness of URL/IP address and must verify the physical location of web server.

g. For System Certificate the HO has to ensure the correctness of MAC/Serial No./IP address of the system.

h. The HO has to put his signature and official seal for verification and the photograph pasted on the form.

C. Guidelines for NIC-Coordinator

On receipt of DSC application form, NIC-Co-ordinator must check & tick the Checklist based on information/documents available with the DSC form before forwarding to NIC RA/CA Office. He/She has to put his signature along with official seal. In case of Class-3 DSC applicant, **Annexure-III** has to be dully filled & submitted.

[Version: DSC Form V 6.2 (Doc-Id. Form-1) Updated on: 25 June 2014]   Page 4

Annexure-I
(Applicant Code & Category)

Code	Category	Code	Category
1.	Govt.	6.	Contractual employee in the above category
2.	Judiciary	7.	MP/MLA
3.	PSU	8.	Elected Member of Village Panchayat/Gram Sabha
4.	Statutory/Autonomous Body	...	...
5.	Sec. 25 Company of Govt.	99.	**Others**

Annexure-II
(Project Code & details)

Code	Project	Code	Project
1.	E-Procurement - NIC portal	21.	Integrated Finance Management System
2.	E-Tendering - NIC portal	22.	Professional Courses Counselling, Admissions & Results
3.	E-Tendering - Others	23.	Public Service Management System (Under the Public Service Commission Act, MP)
4.	E-Courts	24.	e-FMS (Facility Management System Under the MGNREGA)
5.	Supply order placing/DGS&D	25.	UP Technical Education Counselling
6.	E-office	26.	UP Polytechnic Counselling
7.	Income Tax Return Filing	27.	UP B.Ed counselling
8.	Email authentication	28.	UP Medical Counselling
9.	Bhoomi Project	29.	UP VAT (Commercial Tax)
10.	E-District	30.	SSDG/EDS
11.	MNREGA	31.	UP Education Department
12.	Election Commission	32.	Instant Money Order of Deptt of Posts
13.	OASYS (Online Answering Information System for Assembly Questions)	33.	Online Police verification for passport
14.	LRC (Land Record Computerization)	34.	Mee Seva – Government of AP portal.
15.	Treasury (for E-Payment)	35.	ERMS Module - Portal for CEO, Tripura (Election Commission)- private portal
16.	Food & Civil Supplies (for Ration Cards)	36.	Vat Soft for Taxes & Excise Organisation, Govt. of Tripura
17.	Nemmadi - Rural Digital Services	37.	IVFRT
18.	eAPAR	38.	
19.	Health department of Bangalore Mahanagara palike	...	
20.	Web HALRIS and Web HARIS	99.	**Others**

A. Instructions for DSC Applicants

1. NIC-CA abides by the Information Technology Act, 2000, laid down by the Govt. of India. The applicant must read the IT Act 2000 under Resources (https://nicca.nic.in).

2. Subscriber is required to send one copy of DSC request form, duly signed and forwarded by Head of Office to respective RA/NIC-CA. Applicant is advised to retain a copy of the same, which would be required while generating DSC request on line from https://nicca.nic.in

3. The RA/NIC-CA scrutinizes the DSC form, 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. The form will be valid for 90 days only (applicant has to generate key pair request and download certificate within 90 days) failing which, user is required to submit fresh DSC application.

4. It is very important & legally binding to keep the private key securely, for which the applicant must generate key pairs/request using FIPS-140 Level-2 compliant smart card/USB crypto-tokens, which guarantees that private key never leaves the card/token once generated.

5. In case of loss/compromise of DSC, applicant should immediately inform NIC-CA office either by phone 011-24366176 or e-mail at casupport@nic.in or send online revocation request through Member Login from https://nicca.nic.in.

6. For viewing all valid DSCs and CRLs, the user can access the website (https://nicca.nic.in/) under Repository.

7. Smart card/USB crypto-tokens, **allow only maximum 4-10 numbers of incorrect attempts for entering pass phrase/pin**. It is advisable to be careful while entering the pass phrase as repeated incorrect entries shall block the same. On exceeding this limit, special efforts may be required to unblock the device.

8. It is important to note that email-id given by the **applicant is functional** and applicant accesses the same on regular basis as all communication related to DSC like generation, revocation, renewal, expiry details are communicated through the given email-id.

Declaration by Subscriber

I hereby declare and understand that

1. I have read the subscriber agreement under Resource link available on NICCA website (https://nicca.nic.in).
2. I shall keep the private key safe on **FIPS-140 Level-2 compliant smart card/USB crypto-tokens** (Signing/Code Signing certificate) and will not share with others.
3. I shall verify the contents and the correctness of the certificate before accepting the DSC. I shall send a signed mail to NICCA (casupport@nic.in) to acknowledge the acceptance of the DSC.
4. I shall not use the private key before acceptance of the DSC.
5. I authorize NIC-CA to publish the certificate in the NIC-CA repository after acceptance of the DSC.
6. **If the private key of my DSC is compromised, I shall communicate to NICCA without any delay as per the requirement mentioned in Regulation 6 of Information Technology (Certifying Authority) Regulation 2001.**
7. 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.
8. I understand that on cessation of my employment, I shall inform NICCA and my present employer for revocation of my Digital Signature Certificate.
9. 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.
10. **I am aware that Key Escrow/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. I understand that in case of loss of private key of encryption certificate, I will not be able to decrypt the data which was encrypted by corresponding public key of the encryption certificate. I would keep safely backup of p12/pfx encryption key file and recover/restore the same in case its accidental or otherwise loss.**
11. 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.
12. **NICCA shall not be held responsible and no legal proceeding 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.**
13. I am aware that the Certificate, issued by NICCA is valid only for the intended usage and for the period mentioned in the certificate. I undertake not to use the Certificate for any other purpose.
14. I am conversant with PKI technology, and understand the underlying risks and obligations involved in usage of Encryption Certificate/DSC.
15. For SSL Server Certificate, I undertake that I have checked the existence of IP/URL/domain name and physical location of the server.
16. For System Certificate, I undertake that MAC/Serial No./IP No. are correct and are in my custody.
17. For Class-3, certificate I shall appear in person at NICCA/RA/ **Physical Appearance Centre (PAC)** any of the NIC Centres, State Units/ District Centres/Cells at various Ministry Cell of NIC along-with a **photograph** and **departmental photo-id card** for **verification.**
    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 Applicant]**

Verification and/or Declaration by Head of Office of Applicant for issuance of DSC

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.
2. I have verified the credentials of the applicant as per the official records/I have got verification letter from the companies/vendors for the contractual employees from where they have been hired/outsourced, as per the **guidelines given at page 4.**
3. I certify that contractual employee Mr/Ms. _____ is working in project _____ at _____. His/her contract *is valid from* .... to ……….….………..
4. **I hereby** authorize him/her, on behalf of my organization to apply for obtaining DSC from NICCA for the purpose as in DSC.
5. **In case of issuance of encryption certificate**, 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. **I shall not approach NICCA for recovery of private Encryption Key, in case of its loss or otherwise.**
6. For SSL server certificate, I have verified the existence of URL/IP, the IP allocation organisation and physical location of web server.
7. For System Certificate, I have verified the MAC/Serial/IP no of the system/device.
8. It is noted that the organization shall inform NICCA for revocation of DSC on the cessation/superannuation of his/her employment.
9. I have attested applicant's photograph and the copy of the identification proof.

Date:

Place: **[Signature of Officer with Office Seal with name and designation]**

Note: Contractual employees will be issued only signing certificate and with a maximum validity of one year.

Checklist to be ticked [√] by NIC Coordinator before forwarding to NIC RA/CA Office

[ ] All asterisk (*) marked entries are filled   [ ] Payment details filled & DD attached (if required)
[ ] Copy of Departmental photo-Id attested by HO/Service Verification   [ ] Self attested copy of PAN card attached, if any
    letter on letter head with photograph of the applicant
[ ] Signature of Applicant done   [ ] Verification by Head of Office (HO) with Signature & Official Seal
[ ] In person verification is done for Class-3 applicant as attached **Annexure-III** [ ] Affixed photograph attested by the HO

Email:…………………............................ Mobile No.:…………………… **[Signature of NIC Coordinator with name and designation/Office Seal]**
Date: _____   **Place:**_____

[Version: DSC Form V 6.2 (Doc-Id. Form-1) Updated on: 25 June 2014]   Page 2