# IDENTITY VERIFICATION GUIDELINES

Version 1.0

April 15 2015

Controller of Certifying Authorities

Department of Electronics and Information Technology

Ministry of Communications and Information Technology

# Contents

# 1 General guidelines to CAs

i. The guidelines issued by the Controller of Certifying Authorities are to be strictly followed by CAs. Unless and otherwise the date of implementation is specified, the effective date of implementation of guidelines will be from the date of publication on the website of Office of CCA. The changes due to these guidelines should be referred to or incorporated in the subsequent revision of CPS of CAs.

ii. The following text should be part of DSC application form

*Section 71 of IT Act stipulates that if anyone makes a misrepresentation or suppresses any material fact from the CCA or CA for obtaining any DSC such person shall be punishable with imprisonment up to 2 years or with fine up to one lakh rupees or with both*.

iii. The biometric authentication carried out using Aadhaar e-KYC service to establish identity of the applicant, shall be treated as physical verification of subscriber .The (signed) response from UIDAI should be preserved as evidence.

*iv.* CAs should put in measures to ensure that email addresses that are included in Digital Signature Certificates (DSC) are unique to the DSC applicant. Provisions can be made for issuance of multiple DSC with a single email Id where it is established that these multiple DSCs are being issued to a unique DSC applicant.

v. CA should put procedure in place to ensure that no Class 2 or Class 3 individual Signing DSCs are issued in cases where the key pair has not been generated on a FIPS 140-1/2 level validated Hardware cryptographic module.

vi. In respect of Class 1 certificate, if the subscriber prefers to use Non FIPS 140-1/2 Level 2 validated Hardware Cryptographic module/ Software token, the corresponding risk should be made known to the DSC applicant and an undertaking should be taken to the effect that the DSC applicant is aware of the risk associated with storing private keys on a device other than a FIPS 140-1/2 Level 2 validated cryptographic module

vii. A list of approved cryptographic device manufacturers / suppliers and information relating to their FIPS 140-2 validated tokens must be published on the website of the CA.

viii. A digitally signed application form can be accepted for new DSC prior to expiry of existing DSC, provided that CA has infrastructure for archiving such electronic application and validating the signature during the archival period. Identity shall be established through the initial identity-proofing process for each assurance level as per 3.3.1 of India PKI CP.
Also such DSC used to sign the application form should have been issued after Jan 2014.

ix. The application forms shall be preserved and archived by CAs. The archival period of 7 years will begin from the date of expiry of the Digital Signature Certificate.

x. For the purpose of DSC application to CA(paper), all signatures including DSC applicant, attestation and authorisation should be with blue-ink only.

xi. In case applicant's signature is different from that in ID Proof, a physical verification needs to be carried out.

xii. In the case of applicant is unable to sign due to disability, paralysis, or other reasons, the DSC issuance should be through Aadhaar eKYC service.

xiii. Power of attorney is not allowed for the purpose of DSC application to CA and Issuance of DSC.

# 2 Guidelines for issuance of Digital Signature Certificates (Personal/ Organizational Personal DSC)

## 2.1 Personal Digital Signature Certificate – through RAs of CA

1) Registration Authority (RA) is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificate. An RA interacts with the CA and recommends the subscriber request for certificate issuance to CA. A RA should have legal agreement with CA.

2) For issuing a Class 2 DSC, physical verification of original documents against the copy of documents submitted is mandatory before attestation.

3) For issuing a Class 3 DSC, not only the physical verification of original documents against the documents submitted is mandatory but physical verification of person is also compulsory.

4) For all Classes of certificates, other than identity & address proof, the identity credentials which appear in the certificate, like PAN number, e-mail, mobile number etc. as defined in the CPS should be verified.

5) The mobile number of DSC applicant in the DSC application form is mandatory for Class 1, Class 2 and Class3 certificates facilitated through RAs of CAs(other than Banking and organisational). The authentication credentials should be sent to mobile of the applicant. CA should call the subscriber on mobile provided on DSC the application form and confirm that he or she has applied for the DSC. CA should approve the DSC issuance only after the confirmation of DSC applicant.

6) In case of using Aadhaar eKYC based service for verification of individuals, guidelines to be followed is given in the section 5 (Guidelines for e-authentication using Aadhaar e-KYC services).

7) Each applicant for a personal digital signature certificate must provide proof of Identity and proof of address as detailed below:

Document as proof of identity (Any one):

a) Aadhaar (eKYC Service)
b) Passport
c) Driving License
d) PAN Card
e) Post Office ID card
f) Bank Account Passbook containing the photograph and signed by an individual with attestation by the concerned Bank official.

g) Photo ID card issued by the Ministry of Home Affairs of Centre/State Governments.
h) Any Government issued photo ID card bearing the signatures of the individual.

Documents as proof of address (Any one):

a) Aadhaar (eKYC Service)
b) Telephone Bill
c) Electricity Bill
d) Water Bill
e) Gas connection
f) Bank Statements signed by the bank
g) Service Tax/VAT Tax/Sales Tax registration certificate.
h) Driving License (DL)/ Registration certificate (RC)
i) Voter ID Card
j) Passport
k) Property Tax/ Corporation/ Municipal Corporation Receipt

***With the above documents the following conditions will apply.***

I. ***Validation of signature on application forms:*** At least one identity or address proof should contain signature of applicant. If absent, subscribers should submit their signatures validated by the bank where they hold a bank account. The CA/RA should use that verification document to confirm the signature of subscriber present on the application form.

II. ***Validity of the Address Proof:*** In case of any utility bills like electricity, water, gas, and telephone bill, in the name of the applicant , the recent proof, but not earlier than 3 months from the date of application should be attached.

III. ***Using single document copy to be used for both Identity & Address proof:*** This may be considered. However, if the address in the Photo-id is different from the address given in the application then a separate address proof may be insisted for.

IV. ***Attestation against original copy:*** Copy of supporting document should be attested by any one of the following:

- Group 'A' /Group 'B' Gazetted officers (refer Annexure 2)
- Bank Manager/Authorised executive of the Bank
- Post Master

8) DSC shall be issued by CAs only after the application form (with ink signature) and copy of supporting document(s) (duly attested) have been physically received and verified at the CA premises. An officer appointed by each CA, would be responsible for confirming the correctness of the documents provided, before issuing the DSC.
9) For Class 3 Physical verification, a CA should make available a tamper proof video capture facility in their application. The video recording of interactive session with DSC applicant by using the facility provided by CA application should be not less than one minute. The CA should verify the same prior to issuance of DSC to DSC applicant.

## 2.2 Organizational Personal Digital Signature Certificates for officers of Central Government/State Government/PSUs/Autonomous body of Central Government

**Article 12 in The Constitution Of India 1949**
12. the State includes the Government and Parliament of India and the Government and the Legislature of each of the States and all local or other authorities within the territory of India or under the control of the Government of India.

Government organization includes State/ Central Government and their departments, any agency/ instrumentality on which the Government has deep and pervasive control, PSUs, Government Companies, Government Corporations etc.

Identity verification requirements are as mentioned below:

a) Applicant's identity card
b) The application for DSC should be forwarded/Certified by the Head of Office
c) A letter/notification from Head of Department authorizing the Head of Office
d) The attestation of documents may be carried out by Head of the Office/Gazetted Officer
e) For Class 3 certificate HoD should certify the physical verification of subscriber.
f) CA should verify the Organizational and HOD's identity. The identity of HOD should be ascertained by at least one personal interaction, Government ID card, signature and seal of Department, Website RTI disclosures, telephonic call to departmental phone etc.
g) The application forms should be preserved by CA. The electronic application form should be archived in a location provided by CA.

## 2.3 Organizational Personal Digital Signature Certificates for individuals affiliated with Companies/Corporate - Organisation function as RA

1) An organisational RA is an RA who collects and verifies organisational employees/board of directors/partners etc /'s information that are to be entered into his or her public key certificate. An RA interacts with the CA and recommends their organisational person's certificate request information. An organizational RA should have legal agreement with CA.
2) The companies/Corporate should become Organisational RA of CA to obtain DSC for their organisational person. The Organization Name of both applicant and verified organizational RA name should be same.
3) For Class 3 certificate Organization RA should certify the physical verification of DSC applicant.
4) The physical application forms & electronic application form should be archived by CAs.
5) Attested copies the following should be collected and verified by CAs at least once in a year

| **Supporting Documents Existence of organization** | |
|---|---|
| **Category** | **Documents required** |
| Corporate Entities | o Copy of Company Pan Card (Front side page-1)<br>Copy of certificate of incorporation(page-1)<br>o copy of article and memorandum of association(First two page)<br>o Copy of statement of bank account (First and second page)<br>o The copy of audit report along with the annual return pertaining to last financial year (First and second page)<br>o The authorized representatives for forwarding / certifying the application form for DSC should be duly authorized by the resolution of board of directors |

6) The DSC application should be forwarded (with letter) to CA and after the verification by Organisation RA along with copy of organisational person's organisational identity attested/certified by organisation RA

## 2.4 Organizational Personal Digital Signature Certificates for individuals affiliated with companies/corporate or private firms or private firms or partnership firms – through RA of CA

1) Registration Authority (RA) is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her public key certificate. An RA interacts with the CA and recommends the subscriber certificate request information. A RA should have legal agreement with CA.

2) For issuing a Class 2 DSC, physical verification of original documents against the documents submitted is mandatory.

3) For issuing a Class 3 DSC, not only the physical verification of original documents against the documents submitted is mandatory but physical verification of person is also compulsory.

4) For all Classes of certificates, other than identity & address proof, the identity credentials which appear in the certificate, like PAN number, e-mail, mobile number etc. should be verified. In the case of PAN verification, CA should preserve the evidence of verification with their physical / digital signature.

5) The mobile number of DSC applicant in the DSC application form is mandatory for all class of certificates for DSC. The authentication credentials should be sent to mobile of the applicant.
CA should call the subscriber on mobile provided on DSC the application form and confirm that he or she has applied for the DSC. CA should approve the DSC issuance only after the confirmation of DSC applicant.

6) The attestation requirements for Organizational Personal Digital Signature Certificates for individuals affiliated with companies or private firms or private firms or partnership firms through RA are as per annexure 1

7) Only authorized signatories for applying Digital Signature Certificate shall be allowed to apply/forward for DSC application. The authorization requirements form organization for forwarding organization person DSC is given below

| Authorization to Authorized Signatories | |
|---|---|
| **Category** | **Documents required** |
| Individual/Proprietorship Firm: | o The applicant for DSC should be individual/proprietor only |

| | |
|---|---|
| Partnership Firm: | o The *authorized signatories for applying Digital Signature Certificate* should be duly authorized by the partners and his photographs as well as identity and address should be mentioned in the authorization letter. |
| Corporate Entities: | o The *authorized signatories for applying Digital Signature Certificate* should be duly authorized by the resolution of board of directors. The applicant details i.e. address, photograph of the authorized person should also be mentioned in the authorization letter |

8) For each applicant for a organisational person digital signature certificate, the DSC application form should be submitted as detailed below:

.

| **Submission/Forwarding of organizational DSC Application** | |
|---|---|
| **Category** | **Documents required** |
| Individual/Proprietorship Firm: | o The DSC application form should be forwarded by individual/proprietor only |
| Partnership Firm: | o The DSC application should be forwarded by *authorized signatories for applying Digital Signature Certificate* only.<br>o Attested copy of authorization letter *for applying Digital Signature Certificate*<br>o In the case of authorised signatories' self DSC application, It should be counter signed by at least one partner other than authorised signatory. |
| Corporate Entities: | o The DSC application form should be forwarded by authorized representatives only<br>o Attested copy of authorization letter *for applying Digital Signature Certificate*<br>o Attested copy of the applicant's identity card or payroll entry/slip details or organisational identity proof |

9) For each/group of DSC application, the documents required for verification of organizational existence are as mentioned below. All the attested documents specified against the relevant category should be collected and verified by CAs.

| **Supporting Documents in respect of Existence of organization** | |
|---|---|
| **Category** | **Documents required** |
| Individual/Proprietorship Firm | o copy of PAN card (Front side page-1)<br>o Copy of statement of bank account (First and second page)<br>o copy of ITR accompanied by computation of income/financial statement Front side page-1) |

| | |
|---|---|
| Partnership Firm | o Copy of partnership deed ( Max of first three pages including list of partners and authorised signatories)<br>o Copy of PAN card (Front side page-1)<br>o Copy of statement of bank account (First and second page)<br>o copy of ITR accompanied by computation of income/financial statement pertaining to last financial year (First and second page) |
| Corporate Entities | o Copy of Company Pan Card (Front side page-1)<br>Copy of certificate of incorporation(page-1)<br>o copy of article and memorandum of association(First two page)<br>o Copy of statement of bank account (First and second page)<br>o The copy of audit report along with the annual return pertaining to last financial year (First and second page)<br>o The authorized representatives for forwarding / certifying the application form for DSC should be duly authorized by the resolution of board of directors |

10) DSC shall be issued by CAs only after the application form (with ink signature) and copy of supporting document(s) (duly attested) have been physically received and verified at the CA premises. An officer can be appointed by each CA who would be responsible to confirm the correctness of the documents provided, before issuing the DSC.
11) For Class 3 physical verification, a CA should make available a tamper proof video capture facility in CA application. The video recording of interactive session with DSC applicant by using the facility provided by CA application should not be less than one minute. The CA should verify the same prior to issuance of DSC to DSC applicant.

# 3 Guidelines for Issuance of DSC to Foreign Nationals

In respect of Verification of identity credentials of Foreign Nationals applying for Digital Signature Certificates under IT Act 2000, the following method shall be followed.

**Hague Convention/ Apostille Treaty:** is an international treaty drafted by the Hague Conference on Private International Law. It specifies the modalities through which a document issued in one of the signatory countries can be certified for legal purposes in all the other signatory states.

## 3.1 Verification of identity and address documents for foreign nationals

### a. Foreign national is residing in native country

**If native country is a signatory of Hague Convention**: For attestation, proof of identity, address proof and photo on DSC application should be notarized by the Public Notary of that foreign country and **apostilled** by the competent authority of that foreign country**.**

**If native country is not a signatory of Hague Convention:** For attestation, proof of identity ,address proof and photo on DSC application should be notarized by the Public Notary of that foreign country and **consularized** by the competent authority of that foreign country .

Documents required: Passport, Application form with Photo(all attested).

### b. Foreign national residing in India

The following documents should be certified by Individual's Embassy

1. Resident Permit certificate issued by Assistant Foreigner Regional Registration. Officer, an officer of Bureau of Immigration India.
2. Passport
3. Visa
4. Application form with Photo(attested)

### c. Foreign national neither in India nor in the native country

The following documents should be certified by the local embassy of the country to which the person belongs

1. Passport
2. Visa
3. Application form with Photo(attested)

### d. Foreign Nationals holding OCI passport

For foreign nationals with Indian dual citizenship (OCI passport issued by Govt of India and living in India)

1. For DSC with Indian address, the identity and address proof requirements shall be same as Indian nationals living in India.

2. For DSC with foreign address, the copy of their native country passport shall be treated as identity and address proof.

3. No appostilisation and consularisation is required.

4. For DSC application and attestation requirements shall be same as Indian nationals living in India.

5. If applicant not in India then he/she will have to follow the process of a foreign DSC applicant

## 3.2 Organisational person DSC for the categories 3.1 a-c

For organisational person DSC , letter of authorization from organization should be certified in addition to Proof of identity and address of the DSC applicant as given above.

## 3.3 Physical verification of persons for Class 3 DSC for foreign nationals

For Class 3 Physical verification, a CA should make available a tamper proof video capture facility in CA application. The video recording of interactive session with DSC applicant by using the facility provided by CA application should not be less than one minute. The CA should verify the same prior to issuance of DSC to DSC applicant.

# 4 Guidelines for issuance of Special purpose DSCs

## 4.1 SSL Certificates

a) Only authorized organizational persons are entitled to apply for SSL certificates on behalf of an organization.

b) Apart from the organizational person verification, the additional process documentation and authentication requirements for SSL certificate shall include the following:

i. The organization owns the Domain name, or the organization is given the exclusive right and authority to use the Domain Name

ii. Proof that the applicant has the authorization to apply for SSL certificate on behalf of the organization in the asserted capacity.(e.g. Authorisation letter from organization to applicant)

c) A CA shall not issue SSL certificates to any organisational entity unless it owns/controls that domain name.

d) The verification process for applicant's identity (e.g. name, office address, email, etc.), authorization to apply for SSL certificate, and existence of organization should be clearly documented in the CPS without any ambiguity.

e) The documents required for Domain name ownership, proof of existence of organization and authorization to applicant to apply for a SSL certificate are given below.

| Domain Name ownership | |
|---|---|
| **Category** | **Documents required** |
| Individual/Proprietorsship Firm: | Affidavit of ownership in the name of individual or proprietorship firm. |
| Partnership Firm: | Affidavit of ownership in the name of Partnership firm or in the name of |

| | |
|---|---|
| | Partner and in case it is in the name of Partner, additional affidavit from Partner confirming authorisation for use by firm. |
| Corporate Entities: | Certificate of ownership in the name of company issued by statutory Auditor. |
| Government Organisations | Domain Name ownership certified by Head of Office. |

| **Existence of organization (all attested)** | |
|---|---|
| **Category** | **Documents required** |
| Individual/Proprietorship Firm: | o copy of PAN card (Front side page-1)<br>o Copy of statement of bank account (First and second page)<br>o copy of ITR accompanied by computation of income/financial statement Front side page-1) |
| Partnership Firm: | o Copy of partnership deed ( Max of first three pages including list of partners and authorized signatories)<br>o Copy of PAN card (Front side page-1)<br>o Copy of statement of bank account (First and second page)<br>o copy of ITR accompanied by computation of income/financial statement pertaining to last financial year (First and second page) |
| Corporate Entities: | o Copy of Company Pan Card (Front side page-1)<br>Copy of certificate of incorporation(page-1)<br>o copy of article and memorandum of association(First two page)<br>o Copy of statement of bank account (First and second page)<br>o The copy of audit report along with the annual return pertaining to last financial year (First and second page) |
| Government Organisations | o The application for SSL should be forwarded/attested/certified by the Head of Office<br>o Copy of applicant's official identity |

| **Authorization to applicant** | |
|---|---|
| **Category** | **Documents required** |
| Individual/Proprietorsship Firm: | The applicant for SSL certificate should be individual/proprietor only |
| Partnership Firm: | The applicant of SSL certificate should be duly authorized by the partners and his photographs as well as identity and address should be mentioned in the authorization letter |
| Corporate Entities: | The applicant of SSL certificate should be duly authorized by the resolution of board of directors. The applicant details i.e. address, photograph of the authorized person should also be mentioned in the authorization letter |
| Government | SIO/DIO/HOD/NIC-Coordinator to ensure the authenticity of both |

| | |
|---|---|
| Organizations | subscriber and Head of Office. |

12) The CA should verify the information provided through email, phone call and publically verifiable information through internet.
13) The attestation requirements are as per annexure 1

## 4.2 Document Signer Certificate

In continuation to publication of "Document Signer" certificates profile in the "Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act" and Key generation requirements in "X.509 Certificate Policy for India PKI" the following direction is issued for strict compliance:

a) The verification requirements for "existence of the organization" and authorization to applicant shall be same as mentioned in the verification requirements for SSL certificates.
b) The applicant of Document Signer certificate should be a organisational person of that organisation. Attested copy of organisational person's organisational identity should be submitted along with application.
c) The following declarations should be obtained from subscriber in the Document Signer Certificate application form
    i. I hereby declare and understand that Organizational Document Signer Certificate issued to us will be used only for automated signing of documents/information and will not be used in any other context including individual signature.
    ii. I hereby declare that necessary controls have been built in software applications to ensure that there is no misuse
    iii. I hereby declare and understand that the documents/messages authenticated using Organisational Document Signer Certificate issued to us is having organisational accountability.

# 5 Guidelines for e-authentication using Aadhaar e-KYC services

Under the Information Technology Act, Digital Signature Certificates (DSC) are being issued by Certifying Authorities (CA) on successful verification of the identity and address credentials of the applicant. These guidelines are intended to be used to issue DSCs by CAs to DSC applicants who have **Aadhaar Number** with the **email-Id or mobile phone number** registered in UIDAI Database. CAs needs to provide a mechanism to generate DSC application form for DSC applicant based on the biometric authentication through Aadhaar eKYC service. As part of the e-KYC process, the applicant for DSC authorizes UIDAI (through Aadhaar authentication using biometric) to provide their demographic data along with his/her photograph (digitally signed and encrypted) to CAs for verification. The DSC applicant's information received by CAs using Aadhaar eKYC service should be preserved by CA.

a) Applicant's email or mobile numbers are pre-requisites for issuance of Digital Signature Certificate through Aadhaar e-KYC verification channel.
b) CA should be an authorised e-KYC user agency of Unique Identification Authority of India (UIDAI).
c) For all classes of Digital Signature Certificates, to establish identity of the applicant, one or more biometric based authentication should be used.
d) All communication should be through the registered email id or an email id authenticated with challenge password through the registered mobile phone of the applicant.
e) The DSC application form should be generated by submitting Aadhaar number of subscriber and populating the information received from UIDAI and the case the application should be signed by DSC applicant. Additional information like PAN, class of DSC etc should be verified online.
f) Through Aadhaar e-KYC service, UIDAI provides digitally signed information relating to DSC applicant. This contains name, address, email id, mobile phone number, and photo and response code. The response code, which is preserved online for six months by UIDAI and further two years offline, should be recorded on the application form and should also be included in the DSC. CAs should preserve the digitally signed verification information as per the requirements mentioned in the Information Technology Act
g) Any other information which is not part of information received from UIDAI such as PAN etc, that are required to be included in the Digital Signature Certificate, should be verified by CA and the proof of the same should be retained.
h) In the case of organizational person certificates, the DSC application form shall mandatorily populated with the name, photo and response code information received from Aadhaar eKYC services. The remaining information should be filled as per organisation person verification guidelines.

# 6 Guidelines for issuance of Digital Signature Certificates to bank account holders and bank RAs

Digital Signature Certificates (DSC) are being issued on verification of the identity and address of the applicant under the Information Technology Act. These guidelines are intended to be used to issue DSCs by CAs to applicants who have bank accounts and the DSC application is received through the applicant's bank. The bank needs to verify the information retained by bank for establishing the identity of the account holder for opening the bank account against that present in the DSC application form. As the banks follow due-diligence in the verification of identity and address of account holders as per RBI Guidelines, the same verified information can also be used in the DSC application for obtaining a DSC from a Licensed CA.

1) The term **"Banking Registration Authority**" hereafter referred to as **Bank RA** is a branch head/manager in each branch of their Bank, designated for the purpose of validation and recommendation of account holder's information present in their database to apply for a Digital Signature Certificate to a Licensed Certifying Authority. The certificate issued to Banking RA by IDRBT CA should comply with the profile mentioned in Annexure A and is intended only for authentication of Banking RA by a licenced CAs.
2) The Bank RAs are required to retain/archive the DSC application form and be subject to audit in accordance with the audit parameters specified in respect of the information used to obtain DSC which is validated against the information retained in their database. A Bank RA should follow the specific guidelines issued by CCA for issuance of DSC to its account holders. Bank-RAs are subjected to audit as per the auditing checklist specified. As the issuance of DSC to account holder and subsequent usage of DSC for authentication and transaction signing, has direct impact on securing internet banking, banks should take remedial measures on any audit observation immediately. An agreement needs to be executed between Banks and CA.
3) Information retained in the bank database for establishing the identity of account holder for opening the bank account and a certification(Digitally Signed) of the same by a designated Bank RA can be accepted by any Licensed CAs for issuance of DSC to bank account holder . However any other information which is to be present in the DSC should be verified by CA directly or in the process of communication prior to issuance DSC to account holder.
4) To enable issuance of DSC to bank account holder through Bank RA, the Identity and Address proof can be used. If the required information is not present in the bank's database, it should be modified to include the same.
5) After establishing the DSC applicant's credentials from the database of bank, and submission of authenticated electronic request to CA, further issuance steps should be taken care by CAs and their Help Desk. The authenticated electronic request to CA should include IFSC code of the bank so that CA can include IFSC code in the OU field of certificate of account holder. The requirements in respect of certificate issued through bank channel are given in below.
6) For renewal of DSC, Submission of electronic application form by an account holder with valid digital signature is permitted. However it should be necessarily be through same bank.

7) For Class 3 certificate issuance, personal verification is mandatory and the Bank RA should complete the physical verification of applicant before recommendation for Class 3 certificate issuance to CAs.

## 6.1 Security Guidelines for usage of DSC in Banking.

1) For authenticating DSC application form for issuance of DSCs to Banking account holders, Banks RA should use DSC issued by IDRBT CA only. The Banking RA DSC should be of Class III level assurance. As a part of the process of certificate issuance to Bank RAs, a unique serial number (Bank IFSC Code) should be assign to Bank RA and a list of Bank RAs should be made available on IDRBT's site as an optional source of verification by CAs.
2) The designated location of functioning of Bank-RA should be consistent with address details given in the DSC issued to Bank-RA. In the event of transfer of designated Bank-RA, the banking procedures should insist on the revocation of Bank-RA certificate and issue a new certificate to the newly designated Bank-RA.
3) The archival of digitally signed DSC application forms can be undertaken by CAs on the behalf of Banks.
4) The cryptographic token for creating and holding the private credentials is to be made available to the DSC applicant by CAs; however banks can facilitate the DSC issuance by distributing crypto tokens through their own arrangement. Such token should comply with Information Technology Act Standards and guidelines issued by CCA.
5) In order to minimize the manual key-in errors, it is recommended that the account holders information retained by banks are made available to DSC application form which is to be signed and submitted to CA by a Bank RA through automated software programs.
6) In the case of account holder having accounts in multiple banks and obtained DSC through one bank channel or CA directly, the same DSC should be accepted by all banks through a registration process. Prior to acceptance of a DSC, issued another bank, the bank should satisfy themselves through validation of information present in DSC against information kept in their database like Name, address, PAN or Aadhaar Number etc to ascertain that the DSC belongs to the same account holder only. Validity of certificate in respect of revocation and path validation should be carried out prior to acceptance of DSC. To associate customers DSC to Customers bank account, PAN or Aadhaar Number is mandatory in the DSC and the same should have been registered in the Banks' account details also. The banks should reject the DSCs , if they are not satisfied with the association of DSC with customer
7) The banks should direct customers to inform CA as well as all the banks (where DSC is registered for authentication and signing) in the case of lost or stolen tokens or any other revocation scenario . The banks should have a mechanism to remove association of DSC to the subscriber's account immediately.

## Bank RA Certificate Profile (Issued by IDRBT CA)

***Issuer DN***

| Attribute | Value |
|---|---|
| Common Name (CN) | IDRBT CA {Generation Qualifier} {Re-issuance Number} |
| House Identifier | Castle Hills |
| Street Address | Road No. 1, Masab Tank,Hyderabad |
| State / Province | Andhra Pradesh |
| Postal Code | 500 057 |
| Organizational Unit (OU) | Certifying Authority |
| Organization (O) | Institute for Development & Research in Banking Technology |
| Country (C) | IN |

***Subject DN***

| Attribute | Value |
|---|---|
| Common Name (CN) | Joshi |
| House Identifier | 6,CGO Complex |
| Street Address | Lodhi Road |
| State / Province | Delhi |
| Postal Code | 110003 |
| Organizational Unit (OU) | BKID0006048 |
| Organization (O) | Bank of India |
| Country (C) | IN |

## End User Certificate Profile (issued by CA)

### End User Certificate –Subject Specifications

| | | |
|---|---|---|
| 6 | Organisation Unit | Max Length: 64 Characters<br><br>This attribute MUST either contain the name of the department or sub-division of the organisation the person belongs to if the certificate is being issued for official purposes OR must not be used.<br><br>The Organisational unit must not be present when the organisation has been marked as “personal”<br><br>The Organisational unit must be bank IFSC Code when the organisation has been marked as “Banking Personal” |

**Issuer DN**

| Attribute | Value |
|---|---|
| Common Name (CN) | (n)Code Solutions CA {Generation Qualifier} {Re-issuance Number} |
| House Identifier | 301, GNFC Infotower |
| Street Address | Bodakdev, S G Road, Ahmedabad |
| State / Province | Gujarat |
| Postal Code | 380054 |
| Organizational Unit (OU) | Certifying Authority |
| Organization (O) | Gujarat Narmada Valley Fertilizers Company Ltd. |
| Country (C) | IN |

**Subject DN**

| Attribute | Value |
|---|---|
| Common Name (CN) | J Manohar |
| Serial Number | 794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4 |
| State or Province Name | Delhi |
| Postal Code | 110003 |
| Organizational Unit (OU) | BKID0006048 |
| Organization (O) | Banking Personal |
| Country (C) | IN |

# 7 Key Generation

In the context of key pair generation by DSC applicant , if

1. DSC applicant generates key pair in hardware crypto graphic token as specified in the section 6.1.1 of CP and
2. keys are generated in the physical presence of person authorized by CA as witness who certifies the certificate signing request(CSR) to CA using Digital Signature and encrypts the CSR with the public key provided by CA and
3. verification of authorized person's signature and prior to issuance of DSC by CA.

OID 2.16.356.100.10.2 shall be asserted in the policy field of DSC.

# 8 Annexure

**Annexure 1 Attestation**

Copy of supporting document should be attested by ***any one*** of the following:

- Group 'A' /Group 'B' Gazetted officers
- Bank Manager/Authorised executive of the Bank
- Post Master

Important note : The Name, designation, office address and contact number of the attesting officer should be clearly visible. With this, CA should able to trace and contact the attesting officer if required. Only the clear and complete attestation should be accepted by CAs. Attestation is applicable for paper documents only.

**Group 'A' Gazetted officers include**

a) All India services though posted to states
b) Promotes from states to the cadre of Assistant commissioner and above
c) Police officers (Circle Inspector and above)
d) Additional District Civil surgeons
e) Executive Engineers and above
f) District Medical Officer and above
g) Lt. Col and above
h) Principals of Government Colleges and above
i) Readers and above of Universities
j) Patent Examiner etc.

**Group 'B' Gazetted officers include**

a) Section Officer
b) BDO(Block Development Officer)
c) Tahsildar
d) Junior Doctors in Government Hospitals
e) Assistant Executive Engineer
f) Lectures in Government colleges
g) Headmaster of Government high schools
h) 2nd Lieutenant to Major
i) Magistrate

When DSC applicant interacts directly(physical) with CA at CA premises, the attestation of documents as specified above is not required. CA needs to certify the copies against the original.

All electronic verification, such as PAN, should be digitally signed by CA and evidence should be preserved.

## Annexure 2 summary of verification

### SUMMARY OF VERIFICATION

| RA | CERTIFICATE TYPE | IDENTITY PROOF | ADDRESS PROOF | SIGNATURE VERIFICATION BY | TELPHONE VERIFICATION | ATTESTATION | PHYSICAL VERIFICATION BY | ARCHIEVE |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| RA of CA | PERSONAL | PHOTO ID WITH SIG OR eKYC | eKYC or AS PER 2.7 | CA | CA | AS PER ANEXURE 1 | TAMPER PROOF VIDEO | CA |
| | ORG. PERSON | ORG. ID OR eKYC | ORG LETTER | CA | CA | AS PER ANEXURE 1 | TAMPER PROOF VIDEO | CA |
| ORG. RA | ORG. PERSON | ORG. ID OR eKYC | ORG LETTER | ORG RA | ORG RA | ORG RA | ORG RA | CA |
| BANK RA | BANK CUSTOMER | AS IN BANK'S DATABASE | AS IN BANK'S DATABASE | BANK RA | AS IN BANK DATABASE | BANK | BANK RA | BANK RA |
| AADHAR eKYC | PERSONAL | AADHAR eKYC | AADHAR eKYC | NA | **AS IN UIDAI DATABASE | *AS PER ANEX1 OR ORG RA OR CA | NA | CA |
| | ORG. PERSON | AADHAR eKYC | ORG LETTER | NA | **AS IN UIDAI DATABASE | *AS PER ANEX1 OR ORG RA OR CA | NA | CA |

* For individual credentials other than that received through Aadhaar eKYC. In the case of online pan verification, verification and the preservation of digitally signed proof by ca suffice attestation.

** the individuals demographic details information received through Aadhaar eKYC service need not to be re-verified..

**********