IDENTITY VERIFICATION GUIDELINES

Version 1.7

Dec 26 2018

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	IDENTITY VERIFICATION GUIDELINES
Status	Release
Version	1.7
Release Date	Nov 29 2018
Last update	Dec 26 2018
Document Owner	Controller of Certifying Authorities, India

Contents

Definitions

"CA premises" means the location where the Certifying Authority system is located.

"CA Verification Office" means the office owned or leased by CA for the purpose of verification of identification and address of any person requesting a Digital Signature Certificate.

"trusted person" means any person who has:-

a) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or Rules in respect of a Certifying Authority, or

b) duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of a Certifying Authority's computing facilities.

"CA Verification Officers" means trusted person involved in identity and address verification of DSC applicant and approval of issuance of DSC.

"Subscriber Identity Verification method" means the method used for the verification of the information (submitted by subscriber) that is required to be included in the Digital Signature Certificate issued to the subscriber.

"Attestation", for the purpose this document, is defined as certifying copies of document as true copies of the original.

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. DSC application form can be generated by CA based on the verified information held in eKYC account maintained by CA as per section 5 after obtaining the two factor authentication of the applicant.

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 2 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 Level 2 validated tokens must be published on the website of the CA.

viii. The application forms, supporting documents and all other verification information including Video Recording and details of telephonic verification shall be preserved and archived by CAs for a period as mentioned in the IT CA rules, 27. Archival of Digital Signature Certificate is from the date of expiry of the Digital Signature Certificate.

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

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

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

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

xiii. In case of paper based application form , the applicant should affix signature covering Photo and application form

xiv. A CA may ask for more supporting documents, if they are not satisfied with the documents that have been submitted.

xv. The inspection and approval of physical DSC application form should be carried out by a trusted person of CA. Such approval should be clearly indicated on the physical DSC application form in the form of ink signature of trusted person of CA along with name, designation and date. In the case of electronic DSC application form, electronic approval should be with the Digital Signature of trusted person only.

xvi. CA should make sure that the trusted person' roles and responsibilities should not be delegated to or controlled by anyone else. All the CA Verification Officers should be employees of the CA and should have undergone training by CA in respect of verification.

xvii. Incomplete application forms should not be accepted by the CA. CA SHALL NOT accept any Digital signature certificate application forms that do not meet the requirements mentioned in the Identity Verification Guidelines. CA SHALL look for any indication of alteration or falsification in application or supporting documents.

xviii. Application form along with the supporting documents must be available for inspection at CA premises within 30 days of issuance of DSC. In the case of lost DSC application form, the same should be informed to office of CCA within 45 days of issuance with the report of action taken.

xix. DSCs shall be issued by CAs only after the application form (with ink signature) and supporting documents (duly attested) have been physically received and verified at the CA premises/Verification Office.

xx. CAs, for issuing personal DSCs, should mandatorily provide mechanism to apply for DSC directly to CA through their web interface.

xxi. For personal and organisational person DSCs, a letter/certificate issued by bank containing the DSC applicant's information as retained in the Bank database can be accepted. Such letter/certificate should be certified by the Bank Manager. Any information which is required to be part of the DSC but is not a part of such certified letter should be verified by CA. Mobile verification (all applications) and Video Verification will still be required to be done prior to issuance of DSC by CA.

xxii. The eKYC OTP classes of certificates can be used for signing of electronic DSC application form applied from DSC applicant's banking account.

xxiii. In the case of Personal/Organisational Person Digital Signature Certificate issuance (Class 1, Class 2 and Class 3), CA should directly invoice to the DSC applicant or applicant's organisation. CA should carry out periodic reconciliation of invoices raised for DSC issuance with corresponding DSC issued to subscriber. Copy of the invoices issued to DSC applicant should be preserved by CA.

xxiv. For all categories of DSC applicants, it is mandatory to provide either PAN or Aadhaar Number. In the case of PAN or Aadhaar Number not having been issued to a DSC applicant, CA should issue DSC only after obtaining an undertaking from the DSC applicant stating the following.

"I hereby declare that neither PAN nor Aadhaar Number has been issued to me"

xxv. Physical verification of DSC applicant by CA is mandatory prior to issuance of Class 2 & Class 3 DSC.

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

2.1 Personal Digital Signature Certificate – through RAs of CA

1) Registration authority (RA) is an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of subscriber credentials. RA interacts with the CA and submit the applicant's request for certificate issuance to CA. RA should have legally enforceable agreement with CA.

2) The physical verification of person is also compulsory for Class 2 & Class 3 DSCs

3) 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.

4) The mobile number of DSC applicant in the DSC application form is mandatory for Class 1, Class 2 and Class 3 certificates facilitated through RAs of CAs. The authentication credentials will be sent to mobile of the applicant. Prior to issuance of DSC,

   i). The CA should carry out a telephonic verification of the DSC applicant on the mobile number specified in the application form and the recording of same should be stored. CA should log the information as part of audit logs, which shall include Identity of the CA Officer (Name / ID) who conducted the mobile verification and the date and time of the verification.

   OR

   ii). The designated CA system should receive SMS directly from the DSC applicant (from the mobile number specified in the application form). The SMS should contain at least information relating to the DSC Application Number and the Date of birth/email of the DSC applicant and the same should be validated against the details given in the DSC application. The details of SMS (message id, content, applicant mobile number, date and time) should be preserved as part of verification information

   CA should issue DSC only after conducting the telephonic verification or on receipt of the SMS from the DSC applicant.

5) In case of using Aadhaar eKYC service for verification of individuals, guidelines to be followed is given in the section 5.2 (Aadhaar offline eKYC).

6) 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/statement 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 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

Physical verification of original documents against the copy of documents submitted is mandatory before attestation

7) 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 verification Office. A trusted person of each CA, would be responsible for confirming the correctness of the documents provided, before issuing the DSC.

8) For 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 20 seconds. The CA should verify the same prior to issuance of DSC to DSC applicant. CA should not make available option for uploading offline video recording and also should not accept offline recording by any other means.

2.2 Organizational Person Digital Signature Certificates for officers of Central Government/State Government/PSUs/Autonomous body of Central Government /Banks

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) Copy of applicant's identity card or Proof of individuals association with organisation
b) The application for DSC should be forwarded/Certified by the authorized signatory (Competent authority of the Department/ Head of Office / NIC Coordinator….)
c) For Class 3 DSC, Department should certify the physical verification of applicant (with a statement similar to that used for life certificate of pensioners)
d) In case the Department certifies applicant's mobile number, a separate mobile verification is not required.
e) Copy of identity card of authorised signatory or proof of authorised signatory's association with organisation
f) CA should ascertain the identity of authorised signatory by carrying out at least one personal interaction, 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.
h) The activation code should be sent only to the applicant's mobile number.
i) For eGovernance applications, wherever DSCs are issued to stakeholders within Government, DSC activation code can also be facilitated through designated departmental email address. This email ID should be included in the application form and should be identified as a departmental email address.

BANKS

a) The authorization letter with seal and signature, by Bank Manager.(In case of Bank Manager, authorization should be by his/her reporting officer.)
b) copy of Bank PAN Card attested by Bank Manager

c) Certified copy of organizational identity of Bank Manager.
d) The application forms should be preserved by CA.
e) The physical verification of applicant can be certified by Bank Manager.
f) In case the Bank Manager certifies applicant's mobile number, a separate mobile verification through voice call or SMS is not required

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 submits their organisational person's request for certificate. An organizational RA should have legally enforceable 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) Organization RA can 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) Copy of certificate of incorporation(page-1) o copy of article and memorandum of association(First two page) o Copy of statement of bank account (First and second page) o The copy of audit report along with the annual return pertaining to last financial year (First and second page) 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 an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of subscriber credentials. An RA interacts with the CA and submits the subscriber's request for certificate. A RA should have legally enforceable agreement with CA.

2) 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.

3) The mobile number of DSC applicant in the DSC application form is mandatory for Class 1, Class 2 and Class 3 certificates facilitated through RAs of CAs. The authentication credentials will be sent to mobile of the applicant. Prior to issuance of DSC,

   i). The CA should carry out a telephonic verification of the DSC applicant on the mobile number specified in the application form and the recording of same should be stored. CA should log the information as part of audit logs, which shall include Identity of the CA Officer (Name / ID) who conducted the mobile verification and the date and time of the verification.

   OR

   ii). The designated CA system should receive SMS directly from the DSC applicant (from the mobile number specified in the application form). The SMS should contain at least information relating to the DSC Application Number and the Date of birth/email of the DSC applicant and the same should be validated against the details given in the DSC application. The details of SMS (message id, content, applicant mobile number, date and time) should be preserved as part of the verification information.

   CA should issue DSC only after conducting the telephonic verification or on receipt of the SMS from the DSC applicant.

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

5) 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/Proprietor	○ The applicant for DSC should be individual/proprietor only

ship Firm:	
Partnership Firm:	○ 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:	○ 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
Association of person (body of individuals)	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
Limited Liability Partnership	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
Non-Government Organisation /Trust	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

6) In case the company is a single director company with no other authorized signatories, or a proprietorship organization, it can be considered for self-authorization, provided that, necessary undertaking is given on the letter head confirming the reason.

7) 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:	○ The DSC application form should be forwarded by individual/proprietor only
Partnership Firm:	○ The DSC application should be forwarded by *authorized signatories for applying Digital Signature Certificate* only. ○ Attested copy of authorization letter *for applying Digital Signature Certificate* ○ 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:	○ The DSC application form should be forwarded by authorized

	representatives only o Attested copy of authorization letter *for applying Digital Signature Certificate* o Attested copy of the applicant's identity card or payroll entry/slip details or organisational identity proof o In the case of authorised signatories' own DSC application, It should be counter signed by at least one authorised person other than DSC applicant.
Association of person (body of individuals)	o The DSC application should be forwarded by *authorized signatories for applying Digital Signature Certificate* only. o Attested copy of authorization letter *for applying Digital Signature Certificate* o In the case of authorised signatories' self DSC application, It should be counter signed by at least one authorised personal other than authorised signatory.
Limited Liability Partnership	o The DSC application should be forwarded by *authorized signatories for applying Digital Signature Certificate* only. o Attested copy of authorization letter *for applying Digital Signature Certificate* o In the case of authorised signatories' self DSC application, It should be counter signed by at least one authorised personal other than authorised signatory.
Non-Government Organisation /Trust	o The DSC application should be forwarded by *authorized signatories for applying Digital Signature Certificate* only. o Attested copy of authorization letter *for applying Digital Signature Certificate* o In the case of authorised signatories' self DSC application, It should be counter signed by at least one authorised personal other than authorised signatory.

8) 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 Business Registration Certificate" (S&E / VAT / ST) o Copy of statement of bank account (First and second page) o copy of ITR accompanied by computation of income/financial statement (Front side page-1) Note If the individual proprietor does not have proof of Business

	Registration, copy of the PAN Card and copy of the address proof of the Individual/Proprietor should be submitted. In case, the tax return has not been submitted, the Individual/Proprietor should provide a self signed affidavit stating the reason. The bank account should be in the name of organization.
Partnership Firm	o Copy of partnership deed (Max of first three pages including list of partners and authorised signatories) o Copy of PAN card (Front side) o Copy of statement of bank account (First and second page) 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) Copy of certificate of incorporation o copy of article and memorandum of association o Copy of statement of bank account (First and second page) o The copy of audit report along with the annual return pertaining to last financial year (First and second page) o The authorized representatives for forwarding / certifying the application form for DSC should be duly authorized by the resolution of board of directors o Certified copy of organizational ID proof of authorised signatory
Association of person (body of individuals)	○ Copy of PAN Card of entity(Front side) ○ Copy of Incorporation and Registration Certificate issued by authority such as Registrar ○ Copy of Memorandum of Association/copy of rules/Bye laws ○ Copy of Bank Statement(First and second page ○ Copy of Income Tax Return of last year(Front side page-1) ○ Authority/Resolution for Authorization to Authorized Signatories for DSC application/ forwarding/ attestation of organizational documents ○ Certified copy of organizational ID proof of authorized signatory
Limited Liability Partnership	○ Copy of PAN Card of LLP(Front side) ○ Copy of incorporation and Registration Certificate issued by authority such as Registrar ○ Copy of LLP agreement ○ Memorandum of Association/copy of rules/Bye laws ○ Copy of Bank Statement(First and second page) ○ Copy of Income Tax Return of last year(Front side page-1) ○ Authority/Resolution for Authorization to Authorized Signatories for DSC application/ forwarding/ attestation of organizational documents ○ Certified copy of organizational ID proof of authorized signatory
Non-Government Organisation /Trust	○ PAN Card of NGO/Trust(Front side) ○ Incorporation and Registration Certificate issued by authority such as

	Registrar /sub-assurances ○ Copy of Trust Deed ○ Copy of rules and Bye laws of NGO ○ Copy of Bank Statement verified/attested by Banker(First and second page) ○ Copy of Income Tax Return of last year(Front side page-1) ○ Authority/Resolution for Authorization to Authorized Signatories for DSC application/ forwarding/ attestation of organizational documents ○ Certified copy of organizational ID proof of authorised signatory

9) In case tax return is not submitted, the organisation should provide a self affidavit stating the reason.
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/CA verification Office. Trusted person of the CA would be responsible for confirming the correctness of the documents provided, before the DSC is issued.
11) For 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 20 seconds. The CA should verify the same prior to issuance of DSC to DSC applicant.
12) In case organization name is different from that in PAN card, the proof of name change should be submitted.

2.5 Terms and conditions for use of HSM for class 2 or class 3 Organisational Person DSCs.

In the case of DSC (class 2 or class 3) being applied for by Organisational Person, if the key-pairs are proposed to be generated on Hardware Security Module (FIPS 140-1/2 level 3 validated), the certificate signing requests submitted offline may be accepted provided that, along with the DSC application form, a letter of authorization from the authorised signatory of the organisation is enclosed assuring the following.

a. The key pair was generated on a HSM which is under the administrative and physical custody of (Organisation Name) and that signing key activation controls are only with (the DSC applicant Name).
b. The HSM will not be used for any purpose other than for signature by (DSC applicant name).
c. The HSM has been configured to ensure that signing keys generated from HSM are not exportable from the HSM.
d. DSC will be revoked immediately in the event of (the DSC applicant name) quitting or being transferred from (Organisation Name).
e. The following are the details of the HSM being used:
    - make,
    - model
    - unique identification number(s)

3 Guidelines for Issuance of DSC to Foreign Applicant

In respect of Verification of identity credentials of foreign applicant 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 applicant

A DSC applicant is deemed as foreign applicant if the address(residential or organizational) provided in the DSC application form does not belong to India or identity document submitted is not issued by authorities under Government of India.

For the verification of foreign applicant prior to issuance of DSC, the information provided by the DSC applicant in the **DSC application form** such as **Name, photo, signature, residential /organisational address and existence of organisation (if applicable)** must be supported by documents which shall be included as a part of attested/certified documents. If any of these information is not a part of the attested/certified documents, the applicant has to produce additional proof by submitting documents issued by the government/bank of the respective country, in respective of proof of identity (Name, photo & signature) or address (personal/organisational). Such proof shall also be attested/certified

a. Foreign applicant 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/Govt issued identity, Application form with Photo (all attested).

b. Foreign applicant 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 Applicant 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 applicant 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 applicants

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 20 seconds. The CA should verify the same prior to issuance of DSC to DSC applicant.

3.4 Telephone verification

For foreign applicant, mobile verification is exempted and also the activation code can be sent to email ID of the applicant.

3.5 Attestation for applicants

i) The attestation/certification shall be carried out by Apostillization/ Consularization

ii) In case the address included in the DSC application form belongs to a country which is different from the country where identity document has been issued, the 'address proof' should be attested by the attestation authority of the country to which the address belongs

iii) The documents issued by Indian authority can be attested as per attestation requirements mentioned in Annexure 1.

4 Guidelines for issuance of Special purpose DSCs

This section is applicable to the CAs that issue SSL certificates under the special purpose root hierarchy. The pre-requisite for issuance of SSL certificate is that CA should have standalone certificate issuance system for SSL issuance and CAs public key has been certified under special purpose root hierarchy.

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 as per this document only.

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 Business Registration Certificate" (S&E / VAT / ST) o Copy of statement of bank account (First and second page) 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) o Copy of PAN card (Front side page-1) o Copy of statement of bank account (First and second page) 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) Copy of certificate of incorporation(page-1) o copy of article and memorandum of association(First two page) o Copy of statement of bank account (First and second page) o The copy of audit report along with the annual return pertaining to last financial year (First and second page)
Government Organisations	○ The application for SSL should be forwarded/attested/certified by the Head of Office ○ 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.

f) The CA should verify the information provided through email, phone call and publically verifiable information through internet.

g) The attestation requirements are as per annexure 1

h) The CA should verify the Authorization of Domain Name Registrant to use the domain name in the manner given below

Authorization of Domain Name Registrant: CA shall confirm that, as of the date the Registration Certificate was issued, the Applicant either had the right to use, or had control of, the Fully-Qualified Domain Name(s) listed in the Certificate, and was authorized by a person having such right or control to obtain a Certificate containing the Fully-Qualified Domain Name(s).

Third Party Tools: CA shall cross verify the right to use or control the Registered Domain Name(s) from a third party data source like WHOIS.

Authorization of Domain Name if not yet Registered : If domain is not registered in the name of applicant's organization, then the Authorization from the registered owner on the letterhead of owner with a statement granting the Applicant the right to use the Fully-Qualified Domain Name in the Certificate. The CA shall contact registered owner directly, using contact information obtained from a reliable, independent, third-party data source, and obtain confirmation from the Domain Name Registrant that the Domain Authorization is authentic.

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 an 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 maintaining e-KYC account by CA (Only for empanelled ESPs)

Under the Information Technology Act, Digital Signature Certificates (DSC) are being issued by Certifying Authorities (CA) on successful verification of the identity and addresses credentials of the applicant.

5.1 General Guidelines

In all the KYC and account creation processes described under section 5, General guidelines specified in the section 5.1 will be applicable in addition to "1. General Guidelines for CA" unless and otherwise specifically exempted.

I. These guidelines are intended to be used for DSC applicant to have eKYC account with CA based of eKYC of applicant or CA verification. The verified information held by CA will be used for issuance of DSC or eSign.

II. CA to verify the applicant one time and issue DSC subsequently based on 2-factor authentication by applicant. The two factor authentication includes the OTP send to the verified mobile and PIN set by the applicant.

III. Mobile Number of applicant is a pre-requisite for creation of eKYC account by CA for applicant.

IV. As a part of KYC ,before activation, subscriber should set PIN and "user ID"
   a. The eSign Address is in the form "<user-id>@<id-type>.<ESP-id>".
   b. The ESP-ids are eMudhra, nCode, CDAC, Capricorn, NSDLeGov etc. id-types are mobile number, PAN and username.
   c. To ensure ease of use by subscribers, it is recommended that CA should keep user name limited to few characters.
   d. CA shall ensure user IDs is unique within their system.

V. CA should implement security features such as system generated one-time user IDs, temporary locking of accounts, etc.

VI. 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 20 seconds. The video verification should undergo at least two levels, one electronic and one manual level verification, by CA. CA should implement software capabilities to check face in video against photo obtained using KYC or eKYC to perform photo match for electronic verification. For manual check, trusted persons of CA should perform verification for match of photo obtained through eKYC or KYC with the face in video. If automated video verification is not implemented, at least 2 trusted persons should independently verify KYC data against video. CA should not make available option for uploading offline video recording and also should not accept offline recording by any other means.

VII. If PAN of the applicant is to be included in eKYC account for embedding it into the certificate, CA should verify the PAN prior to inclusion in the eKYC account.

VIII. CA trusted person should approve and certify each account information with name timestamp etc and all audits of verification logs should be preserved by CA for seven years from the date of expiry of last certificate issued.

IX. In the case not able to ascertain the genuineness of the e-KYC data submitted by applicant, CA should reject the request and provide option for applicant for direct verification by CA..

X. CA should notify applicant the agreement for the use of KYC information for DSC issuance by CA on successful authentication by the applicant. The applicant should have option to accept or reject the same.

XI. CAs should preserve the digitally signed proof of verification information as per the requirements mentioned in the Information Technology Act.

XII. Applicant should be able to access notifications, history of eSign transactions, account modification etc., activation & deactivation info and also manage any queries/disputes through eKYC account maintained by CA.

XIII. Applicant should have an option to activate, deactivate and close account at any point.

XIV. In the case of change in registered mobile number of subscriber, CA does mobile verification and video verification prior to the register new mobile number in the eKYC account.

XV. Appropriate fraud detection and preventive security mechanisms should be implemented against enrollment frauds.

XVI. CA should have approval of CCA for maintaining eKYC account for applicants.

5.2 Aadhaar offline eKYC

1. It is assumed that subscriber has downloaded digitally signed eKYC XML
2. Subscriber uploads eKYC XML within CA app/website and provides the "share code/phrase" which is used to encrypt the offline KYC XML.
3. CA decrypts XML, validates UIDAI signature, reads the Aadhaar eKYC XML, and extracts demographic data, mobile number (when available), and photo.
4. CA should accept the mobile number within offline KYC only, no changes are allowed.
5. CA optionally captures email for communications, alerts, and PIN reset options. If CA captures email, it must be verified by sending an OTP to email.

6. If PAN of the applicant is to be included in eKYC account for embedding it into the certificate, CA should verify the same prior to inclusion in the eKYC account.
7. Subscriber sets up initial PIN and user ID.
8. CA does interactive video verification(ref 5.1) and also does a photo match of Aadhaar eKYC photo with the video
9. CA should not accept eKYC of the applicant beyond 3 months. The validity of eKYC account will be 2 years for eSign. For DSC issuance, video verification should have carried out within last 3 months

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 I	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 I	IN

End User Certificate Profile (issued by CA)

End User Certificate –Subject Specifications

6	Organisation Unit	Max Length: 64 Characters 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.

		The Organisational unit must not be present when the organisation has been marked as “personal” 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 I	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 I	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.

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. If seal is not visible, the self attested copy of organisational Identity card of attesting officer should be enclosed.

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

Attestation in the case of applicant directly submitting to CAs. When DSC applicant interacts directly (physically) with CA at CA premises, self attested documents can be accepted. CA needs to certify the copies against the original. The proof in respect of site visit by the DSC applicant should be preserved along with application form.

Attestation for existence of organization: The documents related to the existence of organisation can also be attested by authorized signatory/proprietor on the condition that Certified copy of proof of authorized signatory's affiliation to organisation is produced for verification.

Attestation in the case of electronic verification: 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/SMS 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	VIDEO VERIFICATION	CA
	ORG. PERSON(2.3)	ORG. ID OR eKYC	ORG LETTER	CA	CA	AS PER ANEXURE 1	VIDEO VERIFICATION	CA
	GOVT/PSU/BANKS ETC (2.2)	ORG ID PROOF , ORGANISATIONAL LETTER	ORGANISATIONAL LETTER	CA	AUTHORISED PERSON	AUTHORISED PERSON	AUTHORISED PERSON	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 OFFLINE eKYC	PERSONAL	AADHAR eKYC	AADHAR eKYC	NA	**AS IN UIDAI DATABASE	*AS PER ANEX1 OR ORG RA OR CA	VIDEO VERIFICATION	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..

Annexure 3 Change History

Change History

SL	DATE	SECTION	MODIFICATION
1.	21.05.2015	2.1 (5)	Removed (other than Banking and organisational).
2.	21.05.2015	2.1 (9), 2.4 (11) , 3.3	Modified one minutes to 20 seconds
3.	21.07.2015	Annexure 1 - Attestation	In continuation to the text under important notice, the following words to be added " The self attested copy of Id card of attesting officer should be enclosed"
4.	21.07.2015	2.3, 2.4(9), 4.1(e), 2.4(9), 4.1(e),	A) Association of person (body of individuals) B) Limited Liability Partnership C)Non-Government Organisation /Trust Modification "copy of PAN card (Front side page-1)" is replaced with “Business Registration Certificate” (S&E / VAT / ST)"
5.	21.07.2015	Annexure 1 - Attestation	"Existence of organization: The documents related …. Should be provided"
6.	21.07.2015	1 General guidelines to CAs, xiv (new)	In case of paper based application form , the applicant should affix signature covering Photo and application form A CA may ask for more supporting documents , if they are not satisfied.
7.	21.07.2015	2.3, 2.4(9), 4.1(e), -	Note: In case organization name is different from that in PAN card, the proof of name change should be submitted.
8.	21.07.2015	5. 5 Guidelines for e-authentication using Aadhaar e-KYC services	In continuation to "DSC applicants who have Aadhaar Number with the email-Id or mobile phone number registered in UIDAI Database" In case email-Id and mobile phone number is not registered in UIDAI Database, CA can provide a pass code to DSC applicant through application interface after finger Print verification, which can be used as challenge password for further authentication process.
9.	21.07.2015	2.2	Banks Identity verification requirements
10.	11.03.2016	Annexure 1 - Attestation	If seal is not visible, the self attested copy of organisational Identity card of attesting officer should be enclosed.
11.	11.03.2016	Definitions	Definitions added: CA premises, CA Verification office, trusted person, CA verification officers, subscriber identity verification method
12.	11.03.2016	1 General guidelines to CAs,viii, x, xv-xxi(New)	Deleted. 1.viii Modification : existing : …..Blue-ink only modified …… preferably with blue-ink. Modified ix(of earlier version). The application forms, supporting documents and all other verification information including VC and details of telephonic verification shall be preserved and archived by CAsfor a period as mentioned in the IT CA rules, 27. Archival of Digital Signature Certificate from the date of expiry of the Digital Signature Certificate. Clauses 1(xv)-1(xxi) are newly inserted
13.	11.03.2016	2.1 (1),2.3(1)	2.1 (1),: Modified: " Registration authority (RA) is an entity engaged by

		2.1 (5) 2.1 (8)	CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of subscriber credentials. An RA interacts with the CA and submits the subscriber's request for certificate. A RA should have legally enforceable agreement with CA. " (5)(i) Deleted : for two months. (ii) Modified "the audit logs" to " verification information" (8) Existing: CA premises. An officer appointed..... Modified CA verification Office. A trusted person.....
14.	11.03.2016	2.2(a) 2.2(e) 2.2(h)	2.2 (a) & (e) Inserted "or proof of individuals association with organization" 2.2 (h) Added
15.	11.03.2016	2.3(1)	Existing: An RA interacts with the CA and recommends …. Modified: An RA interacts with the CA and submits…….
16.	11.03.2016	2.4(1)	Modified: " Registration authority (RA) is an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of subscriber credentials. An RA interacts with the CA and submits the subscriber's request for certificate. A RA should have legally enforceable agreement with CA. "
17.	11.03.2016	2.4(5)(i)	Deleted : for two months.
18.	11.03.2016	2.4 (8)	Inserted
19.	11.03.2016	2.4(9)	Submission/Forwarding of organizational DSC Application-Corporate Entities Inserted other than DSC applicant at the end of " In the case of authorised signatories' self DSC application,….."
20.	11.03.2016	2.4(10)	Individual/Proprietorship Inserted Note
21.	11.03.2016	2.4(12)	Existing: …….. CA premises. Modified: ……. CA premises/CA verification Office Existing: An officer can be appointed by…… Modified : The trusted person of each CA…….
22.	11.03.2016	3.1 a	Inserted "Govt issued identity" along with passport in the Documents
23.	11.03.2016	3.5	Inserted
24.	11.03.2016	4.1(d)	Modified "clearly mentioned in the cps without any ambiguity" to "as per this document only".
25.	11.03.2016	4.1(h)	Inserted
26.	11.03.2016	Annexure 1-Attestation	1. Under the heading " Attestation in the case of applicant directly submitting to CA",inserted the following "The proof in respect of site visit by the DSC applicant should be preserved along with application form" 2. Under the heading "Attestation for existence of organization" The existing text " …… provided with Certified copy of organizational ID proof of authorized signatory should be provided " has been replaced with " …… on the condition that Certified copy of proof of authorized signatory's affiliation to organisation is produced for verification" 3. Inserted " Attestation in the case of electronic verification "
27.	11.03.2016	FAQ, General 1(a)	Modified RA/CA to CA……
28.	16.04.2016	5.	Aadhaar e-KYC services for e-authentication Section I added

29.	25.07.2016	3.0	3 Nationals has been changed to applicant in 3 3.1 Definition of foreign applicant has been added 3.5 Attestation requirements (i) and (ii) added
30.	25.04.2017	1 General guidelines to CAs	xxiii, xxiv added
31.	25.04.2017	2.5	a new section 2.5 added
32.	25.04.2017	5(g)	Modified
33.	29.06.2017	1 General guidelines to CAs xxiii	Modified
34.	21.07.2017	5. Aadhaar e-KYC services for e-auth	Modification in this section in line with the omission of email and mobile number in Aadhar eKYC response
35.	29.12.2017	1 General guidelines to CAs xxv	Physical verification of DSC applicant by CA prior to issuance of Class 2 personal DSC from 01.03.2018 onwards.
36.	25.05.2918	1 General guidelines to CAs xxv	Physical…… from 01.07.2018 onwards. For Organisational Person DSC, CA should follow the verification procedure for Class 3 in the case of Class 2 DSC also
37.	29.11.2018	1 General guidelines to CAs	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~~. DSC application form can be generated by CA based on the verified information held in eKYC account maintained by CA as per section 5 after obtaining the two factor authentication of the applicant. In the absence of the electronic signature (eSign) on the electronic DSC application form by applicant, ink signature of DSC applicant on a printed DSC application form is required. xi. ~~Aadhaar~~ eKYC ~~service~~ verification. xxi. Verification ~~(Class 3)~~ will xxii ~~Aadhaar~~ eKYC OTP ~~and Biometric~~ xxv Physical verification of DSC applicant by CA is mandatory prior to issuance of Class 2 & Class 3 ~~personal~~ DSC ~~from 01.07.2018 onwards. For Organisational Person DSC, CA should follow the verification procedure for Class 3 in the case of Class 2 DSC also~~
38.	29.11.2018	2.1	2 deleted 3. ~~For issuing a Class 3 DSC, not only the physical verification of original documents against the documents submitted is mandatory but~~. The physical verification of person is also compulsory for Class 2 & Class 3 DSCs 7. under *Attestation against original copy*, added " Physical verification of original documents against the copy of documents submitted is mandatory before attestation" 9 "Class 3" word deleted

39.	29.11.2018	2.2	Under BANKS e. ~~For Class 3 DSC~~
40.	29.11.2018	2.3	3 ~~For Class 3 certificate~~ Organization RA ~~should~~ can
41.	29.11.2018	2.4	2 and 3 deleted 13 Class 3" word deleted
42.	29.11.2018	5	The "5.Aadhaar e-KYC services for e-authentication replaced with "5.Guidelines for maintaining e-KYC account by CA" 5.1 General Guidelines, 5.2 Aadhaar offline KYC - added
43.	26.12.2018	1.0, iii	Removed -: Second sentence removed (In the absence of ... required.
44.	26.12.2018	4.4	Added- (This section is .. hierarchy.)
45.	26.12.2018	5.0	5. heading - added "Only for empanelled ESPs"

Annexure 4 FAQ

FAQ

Frequently Asked Questions on Identity Verification Guidelines Version 1.0

General

1. How the uniqueness of Email ID should be validated?
    a. The CA should ensure that the email ID provided in the application form belongs to the applicant. Further appropriate system checks shall be put by CA to ensure uniqueness of email id.
2. What is the technical validation to be made by CA to ensure uniqueness of email ID?
    a. A minimum validation should happen during application submission that, the given email ID should not have been issued to any other identifier (such as PAN or date of birth). This validation needs to happen for all the historical DSCs issued by the CA for minimum of last 12 months. This will provide reasonable assurance of uniqueness of the email ID provided by the applicant.
3. In case of Signature mismatch with ID proof, it is indicated to perform a physical verification. Should this be made by CA or by RA?
    a. The physical verification in such cases should be made by CA, where the applicant establishes his identity and signs in front of authorized person of CA.
4. It is indicated that, in case of Government Applicants, CA should verify the Organizational and authorised signatory's identity. Is this applicable for Class 3 alone, or even for other classes of certificate?
    a. All classes of certificates.
5. In case of Individual applicant, it is said that “any government issued photo ID card bearing signature of the applicant”. Are government employee ID card acceptable?
    a. The Government Employee ID card is acceptable, only in the cases where it is carrying the central or state emblem. Thus it satisfies as the official card issued by central or state government.
6. In case of Organizational DSC applicant, is there need for Individual address proof?
    a. No.
7. It is specified that, the previous year Audit Report and Annual return (or ITR in case of Partnership / proprietorship) is required as the supporting document for Organizational DSC. What in case the Organization is established recently?
    a. In case the organization is not older than 12 months, this can be excluded. However, all other documents including bank statement remains mandatory.
8. In section 2.1, point 4 of the guidelines, it is indicated that the PAN, email ID, mobile number should be verified. How the email has to be verified? Does a question of email ID in mobile verification process fulfil the requirement, or should an email link should be sent to technically verify before approval of the certificate?
    a. Email should be verified independent of mobile verification. All verification should have been carried out prior to the issuance of DSC. The email should be technically verified.

Attestation Procedures

1. What is attestation?
    a. For the purposes of DSC application, attestation is the procedure where the designated Attestation Officer certifies the photocopy of the document, against satisfactorily ensuring the genuineness of the photocopy (against the original copy).

Usually the attestation bears a seal named “Verified against Original”, which is self-explanatory.

2. Who can attest?
    a. The list of attestation officers is given in the annexure 1 of Verification Guidelines. This includes Group A and B Gazetted Officers, Bank Managers or the Authorized executive of the Bank, and the Post Master.
3. Is self-attestation required?
    a. As digital signature has high potential for misuse, self attestation is not accepted. Only attestations by authorised officials are accepted.
4. How to find / identify a gazetted officer?
    a. The list of designations of Group A and Group B gazetted officers are given in the annexure 1 of Verification Guidelines. These officers are available largely across the country and would be accessible in their respective offices.
5. Is the seal of the attesting officer and date of attestation mandatory?
    a. Yes.
6. Can RA Attest against the originals?
    a. No.
7. How CA has to verify the attestation from Gazetted Officer?
    a. CA has to verify the designation of the Gazetted officer to be in annexure 1 of Verification Guidelines. Additionally, in case of any doubt / randomly, CA should be able to reach out to the officer, in the contact details provided in attestation, and verify the genuineness of attestation.
8. Should CA also check for presence of Name, Designation, Address and Contact number of the attesting officer, in the supporting documents attested?
    a. Yes. These fields are required to be present in at least one of the attestation document, where other documents are attested by same officer.

Mobile Verification

1. Which category of applicants is this applicable?
    a. Unless and otherwise not exempted, all applications received through “Normal RA”,
2. Who should make the call?
    a. The Mobile Verification should happen at CA capacity, where the people designated by CA shall speak to the applicant and verify the information. The verification made by the RA shall not be considered adequate.
3. Can incoming call by applicant be considered?
    a. Yes. However, in case of incoming call, CA should validate that the caller has called from the Mobile number provided in application form. Necessary audit logs shall be available for this purpose.
4. Is the mobile number mandatory for DSC Application?
    a. Yes.
5. Should the mobile number be unique for the given certifying Authority?
    a. Yes.
6. How the uniqueness of Mobile Number should be validated?
    a. The CA should ensure that, they satisfactorily verify with the applicant, that the Mobile Number provided in the application form belongs to them.
7. What is the technical validation to be made by CA to ensure uniqueness of Mobile Number?
    a. A minimum validation should happen during application submission that, the given Mobile Number should not have been issued to any other identifier (such as PAN or date of birth). This validation needs to happen for all the historical DSCs issued by

the CA for minimum of last 12 months. This will provide reasonable assurance of uniqueness of the Mobile Number provided by the applicant.

8. Can Landline number be provided instead of mobile number?
    a. No.
9. What are the basic KYC questions to be verified in Mobile Verification?
    a. Questions of KYC should validate the Applicants Identity, Applicants consent for obtaining DSC, the information provided in application, and the RA information through whom the application was submitted.
10. What details should be logged for Mobile Verification?
    a. For successful mobile verification, CA should log the information as part of audit logs, which shall include, CA Officer Identity (Name / ID) who made the mobile verification, date and time of verification, and other information which were part of application (like applicant name who completed the verification, the mobile number, etc)

Video Recording/Verification

1. Who has to perform the video recording?
    a. The video recording should be done by CA, which can be facilitated by RA. The recording of the video should be real-time and directly in the CA system. There should not be any room for tampering the video or submitting already recorded videos.
2. Is it necessary to make the video recording with applicant to physically be present in CA Premise?
    a. No. It can happen from anywhere.
3. Who has to verify the video recording?
    a. CA has to verify the video recording including the cross verification against the photograph provided in application, the KYC answers stated, etc
4. Can applicant record a video and send it to CA over email, etc?
    a. No.
5. Can the video be recorded in mobile, etc?
    a. The recoding can be facilitated through mobile, only in case where CA has his own mobile application, which can do a real-time streaming to CA System.
6. Can video conferencing solution be used for video recording?
    a. Yes, provided, it satisfies the real-time recording to CA's application.
7. What should be the minimum duration of video recording?
    a. Minimum of 20 Seconds
8. When there is a physical verification through Video recording, what is the need for Attestation of documents?
    a. Attestation is a separate procedure for authenticity of supporting documents. So, it is required irrespective of video verification.
9. In some of the government offices and corporate offices, video recording is not allowed. How to get this Video recording in such case?

    Video recording can be facilitated from anywhere. The applicant can either visit CA / any other location, or fulfil video recording for CA
10. In case of video recording whether mobile phone/SMS verification is required.
    a. Mobile phone/SMS verification is required.

Foreign Applicants

1. Why both "Public Notary" and "Apostillization" is required for foreign national in their native country?

    a. Public Notary is a prerequisite process for Apostillization (or Consularization). This is a common procedure. These are defined in International Law and are governed by various conventions and treaties.
2. How to perform the interactive video recording for foreign nationals, as they are not physically accessible to CA?
    a. CA should facilitate the tamper proof video recording of the applicant. . The video recording with applicant can happen from anywhere
3. What is the allowed address proof, in case the passport of that country does not contain the address?
    a. For the countries, where the address is not the part of passport, the applicant has to produce additional proof of address issued by the government of respective country. Such address proof shall also be certified as applicable.
4. What if the proof of address belongs to some other country? Should that be still attested by respective local embassy?
    a. The 'Address Proof' should be attested by the embassy of the country to which the address belongs.
5. Should the original copy of attested (notarized + appostilled / consularized) document to be submitted?
    a. All certified copies should be with original certification. The photocopy of attested / certified documents shall not be taken.
6. How to verify the notarized + appostilled / consularized procedure?
    a. Appostilled copy will contain the stamp of respective country with clear indication. Consularized copy will bear a stamp and also contain the red tape as per the Consularization process.

Organizational RA

1. Who can be Organizational RA?
    a. As defined in the guidelines, the Corporate Entities or Government Organizations can become "Organizational RA"
2. For whom, an Organizational RA can process a DSC application (issue the certificate)?
    a. They can process the DSC application, only for the employees / directors / etc of their own organization. They cannot issue the DSC to external entities / individuals.
3. What should be the Organizational Name (O Value) in the DSC, for certificates issued through Organizational RA?
    a. The O value in the DSC should be 'fixed' to the Legal name of Organizational RA. All the applications processed through Organizational RA should be an Organizational Personal Certificate, where Organization name cannot be modified.
4. Can an organization procure the DSC through a Normal RA, or is it mandatory for each organization to become an Organizational RA?
    a. Any organization can still procure the DSC through a Normal RA. There is no restriction.
5. In cases of applications through Organizational RA, whether video and mobile verification process is applicable?
    a. No. The Authorized person as defined under Organizational RA Agreement should perform the physical verification, and confirm the data provided in application form.
6. Can an Organizational RA facilitate an Individual Certificate?
    a. No.
7. Can an Organizational RA issue certificate to some other Organizational representative?
    a. No.
8. What kind of agreement should be in place for an organizational RA?

    a. The agreement should mandatorily cover the undertaking of process to be followed as per Organizational RA guidelines. CA or the organization can add additional content on commercials and others.
9. It is said that the KYC of the Organizational RA should happen at least once in a year. What happens in case of 2 / 3 year validity DSC issuance?
    a. This has no relation to the KYC validity of DSC applicant. The DSC once issue will remain valid for the period issued, irrespective of Organizational RA's existence.
10. Can the 'Authorized representative' of Organizational RA, be an external person, who is duly authorized by the Organization?
    a. No.
11. Can a "Normal RA" who is a non-individual and functioning as organization, be treated as an organizational RA?
    a. No.

****