IDENTITY VALIDATION GUIDELINES

sify safescrypt

Version 1.0
May 25 2015

Contents

1 General Guidelines for all Class

i. For the purpose of DSC application to CA (paper), all signatures including DSC subscriber & authorized person should be with **blue-ink** only.

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

iii. Photo ID proof and Address proof can be attested only by Banker, Gazetted officer or Post Master

iv. Email addresses that are included in Digital Signature Certificates (DSC) should be unique. However provisions will be made for issuance of multiple DSC with a single email Id where it is established that these multiple DSC's are being issued to a unique DSC applicant.

v. Power of attorney is not allowed for the purpose of DSC.

vi. 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.

vii. The mobile number of DSC applicant in the DSC application form is mandatory (other than Banking). RA's 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.

viii. DSC shall be issued only after the application form (with ink signature) and copy of supporting document(s) (duly attested) have been physically received .

ix. Each applicant for a personal digital signature certificate must provide proof of Identity and proof of address.

x. 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.

xi. Class 2 or Class 3 individual Signing DSC's key pair has to be generated on a FIPS 140-1/2 level validated Hardware cryptographic module.

xii. 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

xiii. 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.

xiv. 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.

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

Business Registration Document (Any one):

For Corporate Entities:

a) Copy of certificate of incorporation(page-1)
b) Copy of article and memorandum of association(First two page)
c) Copy of statement of bank account (First and second page) attested by the Banker
d) The copy of audit report along with the annual return pertaining to last financial year (First and second page)
e) Copy of Company Pan Card (Front side page-1)

Note: The authorized representatives for forwarding / certifying the application form for DSC should be duly authorized by the resolution of board of directors

For Partnership Firm:

a) Copy of partnership deed (list of partners and authorised signatories)
b) Copy of PAN card (Front side page-1)
c) Copy of statement of bank account (First and second page)
d) copy of ITR accompanied by computation of income/financial statement pertaining to last financial year (First and second page)

For Proprietorship Firm:

a) Sales Tax /VAT Registration document issued to the Sole Proprietorship
b) Copy of PAN card
c) Copy of statement of bank account (First and second page)
d) copy of ITR accompanied by computation of income/financial statement pertaining to last financial year
e) Signature Verification Letter of the Proprietor from the Banker

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:

- Gazetted officers
- Bank Manager/Authorised executive of the Bank
- Post Master

2 For Class 2 & Class 3 DSC:

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

II. **Photo ID** : Government issued Photo ID of the Subscriber which has subscriber signature

III. **Address Proof**: Subscriber address for Individual certificate and Organisational address is required for digital certificate with organisation.

IV. **Proof of Right to do business** : Business registration document is required for Organisational certificate

V. 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.

VI. 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.

VII. For Class 3 Physical verification and the video recording of interactive session with DSC applicant should be not less than one minute.

VIII. 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).

3 For Government Officers:

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) Subscriber’s identity card

b) The subscription form 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 subscription forms should be preserved by CA. The electronic application form should be archived in a location provided by CA.

4 For 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.

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

For organizational 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.

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.

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

Under the Information Technology Act, Digital Signature Certificates (DSC) is 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 DSC's by CA's to DSC applicants who have **Aadhaar Number** with the **email-Id or mobile phone number** registered in UIDAI Database. CA's 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 CA's for verification. The DSC applicant's information received by CA's 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. CA's 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 For Bank RA's and Bank account holders

Digital Signature Certificates (DSC) is 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 DSC's by CA's 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 licensed CA's.
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 CA's 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 CA's 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 CA's.

6.1 Security Guidelines for usage of DSC in Banking.

1) For authenticating DSC application form for issuance of DSC's to Banking account holders, Banks RA should use DSC issued by licensed 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 CA's.
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 CA's 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 CA’s; 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 DSC’s , 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.