IDENTITY VERIFICATION GUIDELINES

Version 1.0

Controller:

Nepal Government
OFFICE OF CONTROLLER OF CERTIFICATION
Ministry of Communications and Information Technology
Singhdurbar, Kathmnadu, Nepal
2079

Document Control

Document Name	IDENTITY VERIFICATION GUIDELINES
Status	Release
Version	1.0
Release	June 2022
Document Owner	Office of Controller of Certification, Nepal

TABLE OF CONTENT

Definitions

"CA premises" means the location where the Certifying Authority Certificate issuance systems are located.

"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 the 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.

1. Guidelines to CAs

Under the Electronic Transaction Act, Digital Signature Certificates (DSC) are being issued by Certifying Authorities (CA) on successful verification of the identity and addresses credentials of the applicant. The guidelines issued by the Office of Controller of Certification are to be strictly followed by CAS.

1.1 General

- 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 the Office of OCC. The changes due to these guidelines shall be referred to or incorporated in the subsequent revision of the CPS of CAs.

- CA shall make sure the following text shall be displayed to the user before submission/signing of the DSC application form

- The eKYC information collected from the applicant shall not be shared by CA and comply with all the provisions of the Electronic Transaction Act for protecting the information

- The subscriber's registered information with CA such as video, photo, ID cards, phone number, PAN/NID, other information submitted and not a part of the certificate in the readable form is confidential and its access shall be limited to only authorized CA personnel.

- Access, sharing, photographic images/video, and/or retention of such information by anybody other than CA, as applicable under the provisions of the Electronic Transaction Act, shall be liable for the penalty for breach of confidentiality and privacy.

1.2 eKYC Account

- A DSC applicant must have an eKYC account before they may apply for a DSC or use the eSign service. The confirmed data kept by CA must be utilized to issue DSCs only. No eKYC account is needed for the eSign service based on online NID authentication.

- The eKYC account of the DSC applicant shall be created by CA based on the eKYC of the applicant (Bank, Organizational, PAN, and Offline/Online NID) or a direct verification (Foreign Nationals). Before activating the eKYC account, the eKYC applicant must submit and have confirmed by CA any information that is needed in the DSC application form but is not included in the applicant's eKYC.

- The eKYC account holder must go through all the verification processes listed for the additional eKYC option if they need more than one account (personal and organizational, for example). The CA should treat the eKYC applicant's two eKYC accounts as belonging to just one eKYC account. The mobile number and PAN can be the same. CA must offer a choice between personal and organizational account modes for user authentication.

- The validity of eKYC account shall not be more than 2 years. The account (with the same username, PAN, Mobile) can be extended only by carrying a fresh verification of the applicant under these guidelines.

- If CA cannot verify the validity of the e-KYC information provided by the applicant, CA must deny the request.

- Upon successful application authentication, CA shall inform the applicant of the subscriber agreement for the use of KYC information for DSC issuance by CA. Whether to accept or reject the offer is up to the applicant.

- The applicant will have access to alerts, eSign transaction history, account modification information, activation and deactivation details, as well as manage any inquiries or disputes through an eKYC account kept by the CA.

- Applicant shall have an option to activate, deactivate, and close account at any point.

- To combat enrollment scams, appropriate fraud detection and preventive security procedures must be put in place. The CA must specifically ensure that the page capturing PIN is secure against threats like phishing attempts, malicious plug-ins, hijack clicks and keystrokes, etc.

- OCC must give CA permission before CA keeps an eKYC account for applicants.

- Resetting the PIN requires both email and a mobile OTP. In the absence of email, it shall be mobile OTP and video verification. When it comes to banking, the PIN reset will only be permitted following a successful match between new eKYC and the registered eKYC details.

1.3 DSC Application Form

After acquiring the applicant's two-factor authentication, CA will construct the DSC application form based on the validated information in its eKYC account.

The DSC application form must have the applicant's electronic signature attached utilizing the CA's eSign program.

Power of attorney is not permitted while applying for and receiving a DSC from the CA.

- If a CA is dissatisfied with the supporting documents provided, they may request more ones.

1.4 Mandatory Information in the DSC application Form

- Name, address (residence/organization), email, Mobile Number, PAN/NID, Photo, Date, type certificate (personal/organizational), the signature of applicant, and Class are mandatory in the eKYC account and DSC application form for issuance of DSC. Email is not required when creating an eKYC account that will solely be used for eSign.
- It is a requirement for all DSC applicants to present either a PAN or an NID number.

1.5 Name

- The DSC applicant's name must match the name on the corresponding eKYC.
- A copy of at least one identity document with a photograph and the applicant's name, as listed in Annexure IV, must be submitted as proof of identity.

1.6Address

- The DSC applicant's address must be either residential or business-related.
- The list of acceptable documents for address proof is provided in Annexure IV.

1.7 Mobile Number

- CA for Mobile Number of applicants is a pre-requisite for the creation of an eKYC account by CA for the applicant.
- The CA must issue an SMS OTP as evidence of ownership of the mobile number, and this proof must be captured using the CA-provided interface. Such verification OTP shall be random, communicated only to the mobile number under verification, and shall not be based on any predetermined parameters to avoid compromise.
-

1.8 Email address

- Email id of the applicant is mandatory for issuance of DSC based on the eKYC account activated by CA. For eKYC accounts that are only active for this purpose, email identification is optional.

- CAs shall 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 the issuance of multiple DSC with a single email Id where it is established that these multiple DSCs are being issued to the same DSC applicant

- For email verification, CA shall send an email OTP or challenge-response or verification URL to the email of the DSC applicant and verify the response through the interface provided by CA. Such verification factors shall be random, communicated only to the email ID under verification, and shall not be based on any predetermined parameters to avoid the compromise. CA should preserve the proof of verification with their digital signature.

- No disposable email (fast temporary email without registration) shall be accepted by CA.

1.9PAN

- Through the eKYC service, CA must electronically compare the PAN number with the Income-tax database and accept only if the name matches exactly. CA must keep the verification proof along with their digital signature.

1.10 Verification

- To establish an eKYC account with CA for the issuing of a design or DSC, an eKYC applicant must electronically verify their identity and the information they provided.

- The verification requirements may vary depending on the source of eKYC like NID, Bank, or organization.

Only the automatic populating of digitally signed information from an eKYC source, such as a bank or NID, in an electronic application form is permitted by CA. The information obtained from the additional source (such as PAN) must only be used to cross-verify the data that the applicant has entered into the CA interface.

1.11 Physical verification/Video verification/online NID eKYC

- The physical verification of the DSC applicant shall be carried out using online interactive video verification directly by CA as per Annexure VI or by an on-line NID eKYC.
- Regardless of the first method of in-person verification, CA must conduct a photo match of an application with that in CA eKYC records during the following verification.
- Any suggestion that a video recording has been altered or falsified must be investigated by the CA.

1.12 Documents verification

The CA shall verify the uploaded supporting documents using direct online interactive video verification of the original documents held by the DSC applicant or online verification from the source of issuance of the documents, in place of the attestation of documents that are present in the paper-based DSC application.

- If applicable, the originals of the identity and address proof shall be verified during the video verification.

- The video verification of the original documents shall be carried out as per Annexure VI

- Using online verification, CA shall verify the authenticity of the document submitted and the digitally signed proof of the online verification shall be maintained.

1.13 Key pair generation/Storage

- As stated in "Storage of Private Key Used by Subscribers for Creating Digital Signatures Guidelines," CA shall issue class 3 level individual signing certificates (both personal and organizational) to the private key generated on a FIPS 140-2 level 2/3 validated Hardware cryptographic module (crypto tokens) or provide as a soft token in an authenticated email. Class 3 individual signing certificates with a combination of class 2 & class 3 certificates by incorporating Class 2 OID in the Class 3 certificates shall be issued by CA instead of class 2 level individual signing certificates alone. Class 2 and class 3 individual signing certificates are equally recognized as class 3 individual signing certificates.

- The CA must implement a mechanism to make sure that no Class 3 individual Signing DSCs are made when the key pair was not created on a FIPS 140-2 level 2/3 verified Hardware cryptographic module (crypto tokens).

- For the protection of crypto tokens against "PIN reset compromise", CA shall follow any of the following options.–

a) Unless the subscriber's crypto-token is re-initialized or formatted, CA shall not support the PIN reset method. In these situations, CA shall re-issue the certificate for the remainder of VA, the certificate's validity, for the convenience of DSC applicants. At least once every certificate, this free re-issuance must be offered. Additional re-issuance may be provided by CA, albeit at an additional cost to the user. After the subscriber has been authenticated, only then may CA carry out this re-issuance.

b) The resetting password of the subscriber for access to the file system of PKI Crypto device/Crypto token by Admin shall be carried out directly by CA. CA shall be the single point of contact for the applicant in respect of crypto token management software/upgrading firmware/resetting passwords etc.

- In respect of Class 1 certificate, if the subscriber prefers to use software Cryptographic module, the corresponding risk shall be made known to the DSC applicant and an undertaking shall 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 140-2 Level 2/3 validated cryptographic module.

- Terms and conditions for use of HSM for class 3 Organizational Person DSCs on FIPS 140-2

level 2/3 certified HSMs shall be as per annexure II.

1.14 Invoice/Acknowledgement

- When issuing Personal/Organizational Person Digital Signature Certificates (Class 1, Class 2, and Class 3), CA must send the DSC applicant or applicant's organization a direct invoice or acknowledgement of DSC issue. Periodically, CA must compare the invoice/acknowledgement with the corresponding DSC given to the subscriber. The CA must save a copy of the invoice or acknowledgment sent to the DSC applicant.

1.15 Subscriber Agreement

- CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.

- For eKYC account creation based on the KYC information source such as Offline NID KYC, Banking, and organizational, the design of the subscriber shall be based on the information received from the KYC information source.

1.16 DSC Issuance

- Only after meeting the verification standards listed in the corresponding eKYC parts of this document will DSC be provided. The maximum period of time for downloading DSC is 30 days from the day that verification and approval were finished. The appropriate verification requirements mentioned in the corresponding eKYC sections of this document shall be carried out by CA prior to DSC issuing if the applicant does not download the DSC within 30 days.

1.17 Archival

- According to the standards outlined in the Electronic Transaction Act, CAs are required to maintain the digitally signed papers, proof of verification data, logs, etc..

- Information must be stored for seven years after the digital signature certificate expires.

1.18 Role of Trusted person

- CA shall make sure that the CA Verification Officer's roles and responsibilities are not be

- delegated or controlled by anyone else.

- All the CA Verification Officers shall be exclusive employees of the CA and shall not have any current or planned financial, legal or other relationship with any external entity facilitating DSC issuance.

- CA trusted person/Verification Officer shall approve and certify each account information including name timestamp etc. using their own digital signature.

1.19 Special purpose certificates

- Apart from the details required for the creation of an eKYC account, the additional details shall be verified by CA following the type of special-purpose certificate.

- Only organizational persons are allowed to apply for a special purpose certificate.

- CA shall verify all the information to have appeared in the certificate and the proof of verification shall be retained. Information that is not verified shall not be included in certificates.

1.20 Encryption Certificate

- The encryption keys and certificates shall be preserved by a subscriber

1.21 First-factor Authentication

- The first-factor authentication to the eKYC account shall be PIN

1.22 Second-factor Authentication

- The second-factor authentication can be SMS-OTP or the other authentication mode specified in the eSign API

- The eKYC account shall be activated using PIN and OTP. Subsequently, other authentication can be used in place of OTP however OTP shall be retained as a fallback option.

1.23 SMS-OTP

- CA shall always send OTP to the eKYC account holder with PURPOSE relevant to the authentication seeking.
- OTP shall be sent only to the verified mobile number registered in the eKYC account.

2. Guidelines for maintaining an e-KYC account by CA

- In all the KYC and account creation processes, these section 1 will be applicable unless and otherwise specifically exempted.

2.1 Authentication for eKYC Account

- CA to verify the applicant one time and issue DSC subsequently based on 2-factor authentication by the applicant. The two-factor authentication includes the PIN set by the applicant and a second factor, as permitted by the guidelines issued by OCC. (Eg: OTP sent to the verified mobile).

- As a part of KYC, before activation, subscriber shall set PIN and "user ID"

a) The eSign Address is in the form "<user-id>@<id-type>. <ESP-id>".
b) The ESP-ids are …… CA etc. id-types are mobile number, PAN and username, etc.
c) To ensure ease of use by subscribers, it is recommended that CA shall keep user name limited to a few characters.
d) CA shall ensure the username is unique within their system. For Personal eKYC accounts, the mobile number and PAN shall be unique.

2.2 NID eKYC

- These guidelines are intended to be used to create eKYC accounts that have a NID Number registered in NIDMC Database or equivalent authenticated database.

- CAs are required to follow the requirements specified by NIDMC strictly for eKYC authentication of DSC applicant

- As part of the e-KYC process prescribed by NIDMC under the NID Act, the applicant for DSC authorizes CA (through NID eKYC) to obtain their demographic data along with his/her photograph (digitally signed and encrypted) to CAs for verification.

2.2.1 NID online eKYC

- This section is allowed as per the provision of NID e-KYC authentication by Certifying Authorities under the OCC for the issue of a Digital Signature Certificate (DSC).

- CA shall be an authorized e-KYC User Agency (KUA if available and when available) of the

Unique Identification Authority of Nepal (NIDMC).

- CA shall provide a direct interface for capturing information required for e-KYC services of NIDMC

- Subscriber shall submit NID Number and perform Biometric/OTP eKYC authentication to NIDMC through the interface provided by CA only.

- Up on the receipt of NID eKYC XML from NIDMC, CA decrypts, validates NIDMC signature, reads and extracts demographic data, and photos.

- The verified information received through online NID e-KYC shall be used for the creation eKYC account of the user.

- The DSC application form should be generated by populating the information received from NIDMC.

- The application should be signed by the DSC applicant. The verified information received through eKYC services can be used for obtaining the design of DSC applicants by CA through a separate user eKYC authentication.

- If the PAN of the applicant is to be included in the eKYC account for embedding it in the certificate, CA shall verify the same before inclusion in the eKYC account.

- On successful NID eKYC Authentication for the eKYC Account, CA shall store the unique UID Token for that NID holder against such eKYC Account. This shall be used for referring to the same user during any re-verification requirements.

- For DSC issuance, an email shall be included in the eKYC account after verification by CA.

- CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.

2.2.2NID online eKYC – OTP

- Subscriber submits NID Number and performs provides OTP authentication through the interface provided by CA to NIDMC.

- Up on Successful authentication, CA receive NID e-KYC XML and create an e-KYC account for the applicant.

- The mobile number is mandatory. CA shall capture the mobile number of the user and carry out verification of the Mobile Number.

- CA does interactive video verification (Annexure VI) and also does a photo match of the

NID eKYC photo with the video.

- For each DSC issuance, video verification shall have been carried out within the last 2 days. The in-person verification can also be substituted by NID Biometric Authentication.

2.2.3 NID online eKYC – Biometric

- Subscriber submits NID Number and performs biometric authentication through the interface provided by CA to NIDMC.

- Up on successful authentication, CA receives NID e-KYC XML and creates an e-KYC account for the applicant.

- The mobile number is mandatory. CA shall capture the mobile number of the applicant and carry out verification of Mobile Number.

- For each DSC issuance, NID eKYC Biometric authentication of an applicant shall have been carried out within the last 2 days and CA should accept only if the face in NID Photo matches against that in the CA eKYC record of the same applicant. The in-person verification can also be substituted by interactive video verification (Annexure VI) provided that CA should successfully verify the matching face in the video with the photograph of the eKYC record of the same applicant.

2.2.4 NID offline eKYC

- It is assumed that subscriber has downloaded digitally signed eKYC XML
- Subscriber uploads eKYC XML within CA app/website and provides the "share code/phrase" which is used to encrypt the offline KYC XML.

- CA decrypts XML, validates NIDMC signature, reads the NID eKYC XML, and extracts demographic data, mobile number (when available), and photo

- CA shall accept the mobile number within offline KYC only, no changes are allowed.
- For issuance of DSC, CA captures email for communications, alerts, and PIN reset options and it must be verified.

- If the PAN of the applicant is to be included in the eKYC account for embedding it into the certificate, CA shall verify the same before inclusion in the eKYC account.

- Subscriber sets up an initial PIN and user ID.
- CA does interactive video verification (Annexure VI) and also does a photo match of the the NID eKYC photo with the video.

- For each DSC issuance, video verification shall have been carried out within the last 2 days. The in-person verification can also be substituted by NID eKYC Biometric Authentication provided that CA successfully verifies the face in NID Photo against that in the KYC record.

- CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.

2.3 Organizational KYC for Organizational Person Certificates

This section is applicable for eKYC applicants affiliated with organizations

- For the organizational person certificate, the Organization Name (O Value) in the certificate shall match the organization name and also comply with the naming convention specified by OCC-IOG.

- The minimum requirements for Issuance of DSC to organization person include

a) eKYC account of Applicant
b) Applicant ID Proof or Proof of individuals associated with organization
c) Letter of Authorization by Organization to Authorized Signatory for self-authorization and also to other DSC applicants.
d) eKYC account of Authorized Signatory and authorization to DSC applicant
e) Proof of the existence of organization

- CA shall carry out the verification of the existence of organization & authorized signatory of
- the organization as per 2.3.1. All the information submitted by eKYC applicant for the eKYC account shall be digitally signed by the authorized signatory.

- The criteria for the eligibility of a government organization and its authorized signatory are
- given in annexure V.

- KYC of organizational eKYC applicant shall be submitted to CA and CA to carry out the verification.

- The eKYC account request shall include Name, Office address, photo, PAN, mobile no, Organizational ID, email, etc. The mobile number and PAN of the applicants are mandatory. The copy of the organizational ID card and PAN shall also be submitted to CA.

- CA shall carry out interactive video verification as per Annexure VI and shall verify the photo
- match of the eKYC photo with the video. The original document verification is also a part of video verification.
- CA activates eKYC account after mobile, email, and PAN verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.

- CA shall provide Organizational eKYC applicant to set up a PIN and user ID upon the authentication by CA.

- In case of any change in the account holder's status or information, the change request shall be submitted with the authorization of the authorized signatory.

- CA shall accept the mobile number within Organizational KYC only, no changes are allowed.

- For DSC issuance, the video verification shall have been carried out within the last 2 days

2.3.1 Verification of Authorized Signatory

- The scanned copy of the documents for the existence of organization & authorization to authorized signatories as per Annexure I of IVG shall be submitted to CA and the originals shall be verified during video verification.

- The steps 4-7 of 2.3 shall be followed for the verification before the eKYC account creation.

- CA shall carry out secondary verification like face-to-face interaction/website reference/call to organizational telephone numbers to confirm the organizational identity of the authorized person and the proof of the verification shall be maintained.

- The steps 8-9 of 2.3 shall be applicable for the eKYC account creation.

- Upon successful confirmation of the organizational identity of an authorized person, CA shall create an eKYC account and may issue DSC to the authorized signatory. The DSC/eKYC Account of the authorized signatory shall be registered with CA and shall be mapped with the name of the verified organization. Subsequently, all the information submitted by the eKYC applicant for the eKYC account shall be digitally signed by the authorized signatory.

- 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 Information is verified on OCR Website (on availability). In the case of a proprietorship organization where the applicant himself/herself is the proprietorship, self-authorization / no authorization is required.

2.4 Banking eKYC for Banking Customers

- This section is applicable only for persons having a Banking account and Banks submit the KYC of the Banking Customer to CA directly after obtaining consent and authentication from the customer. The video verification is not mandatory.

- CA shall verify the source of the request and signature of the bank before accepting KYC information
- CA shall have an agreement/undertaking with Bank.

- CA shall carry out verification of the existence of the Bank, authorized signatory's identity as mentioned in Annexure I of the Identity Verification guidelines
- The DSC to be used for signature by the bank shall be registered with CA and shall be mapped with the bank ID/Name

- The KYC details shall include Name, address, photo, PAN/NID Number, mobile no, Bank account Number.

- The mobile number and PAN/NID Number (last four digits) of the applicants are
- Mandatory

- CA shall allow eKYC applicants to set a PIN and user ID up on the authentication by CA

- CA activates the eKYC account after mobile verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.

- 10.CA shall accept the mobile number within bank KYC only, no changes are allowed.

- 11. For each DSC issuance, CA shall have received the KYC of the account holder from the Bank within the last 24 hours.

2.5 PAN eKYC for Personal Certificates

- This section applies only to persons who submit the PAN & other KYC information to CA directly.
- The mobile number, PAN of the applicant, and Government ID having address (Annexure-IV)
- are mandatory. The scanned copy of the PAN card and Government ID having address shall be submitted to CA

- CA shall carry out verification of Mobile Number and PAN (eKYC). Email shall be captured and verified for DSC issuance.

- The video verification of the applicant shall be carried out by CA as per Annexure VI. During the video verification, the applicant shall display the original PAN card and Government ID having an address for cross verification by CA. Both the PAN details and address in the Id captured in the video shall be in a clear and readable form.

- CA shall electronically verify the PAN number with the Income tax database through the eKYC service and accept only if the name is matching correctly. The digitally signed proof of the verified response shall be preserved by CA.

- CA shall verify the Government ID having address submitted to CA against the original displayed during the video verification.

- The eKYC account request shall include Name (as in PAN), residential address (as in

address id), photo, PAN, mobile no, email etc.

- CA activates the eKYC account after mobile, email, PAN, and video verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.

- In case of any change in account holder's information after activation of an account, CA shall carry out fresh enrollment.

- CA shall allow eKYC applicant to set PIN and user ID up on the authentication by CA.

- For DSC issuance, video verification shall have carried out within the last 2 days. The in-person verification can also be substituted by NID eKYC Biometric Authentication provided that CA successfully verifies the face in NID Photo against that in the KYC record.

2.6 eKYC for foreign applicants

- This section is applicable only for foreign applicants who submit the KYC information to CA directly. An applicant is deemed as a foreign applicant if the address (residential or organizational) provided in the DSC application form does not belong to Nepal or the identity document submitted is not issued by authorities under the Government of Nepal.

- For all categories of applicants, email id, mobile number, photo, scanned copy of proof of identity, and scanned copy of proof of address are required to be submitted to CA.

➢ **For organizational person certificate**

a) Scanned copy of organizational id, organizational email id, mobile number, organizational address, and letter of authorization from the organization is required.

b) For the proof of organizational existence, publicly verifiable and listed/recognized by local government reference of organization in database/registry shall be provided.

c) If the organization is already registered/empaneled in government organizations of Nepal, then the scanned copy of the letter of request issued from the Nepal government organization with the details of the DSC applicant can be accepted as address proof/existence of organization for DSC issuance.

➢ **For Personal certificate**

a) For identity proof, the scanned copy of Passport/Local Govt issued identity/PAN/OCI passport can be submitted.

b) For the address proof the scanned copy of passport/OCI passport/local government-issued id having address/bank details having address/any utility bills in the name of applicant issued within three months/ document issued from the embassy with residential address can be provided

- The video verification shall be carried out by CA as per Annexure VI. All the originals shall be verified during the video verification. The telephonic verification shall be carried out by direct call to the applicant or SMS OTP verification and the proof of verification shall be recorded. Email shall also be verified by CA.

- For telephonic verification, CA can also verify over telephonic call, where CA originates to or receives the call from the mobile number under verification, and validates the number holder with at least 2 questions establishing relation to DSC application

- CA activates eKYC account after mobile, email, PAN (if submitted) and video verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.

- In case of any change in account holder's information after activation of an account, CA shall carry out a fresh enrollment.

- CA shall allow eKYC applicants to set PIN and user ID up on the authentication by CA. The OTP can be sent to the email of the eKYC user.

- During the validity period of the eKYC account, a fresh video verification shall have been carried out for each DSC issuance within the last 2 days.

- For issuance of Document Signer Certificate, the declarations to be obtained from subscriber shall be as per 3.2. (2)

3. Guidelines for issuance of Special purpo se DSCs

This section applies to the CAs that issue SSL certificates under the special purpose root hierarchy. The pre-requisite for issuance of an SSL certificate is that CA shall have a standalone certificate issuance system for SSL issuance and CAs public key has been certified under a special purpose root hierarchy. eKYC account of the applicant is mandatory.

a. SSL Certificates

The issuances of SSL certificates by Licensed CAs are limited only to.NP domain. Only organizational persons are eligible to apply for SSL certificates on behalf of their organizations. The applicant (requestor) shall make an application to the CA in a digitally signed application form. This shall contain the domain name(s) to be certified, the Certificate Signing Request (CSR), and the information of the requestor and the organization. This shall be accompanied by necessary supporting documents. The minimum set of documents to be submitted includes:

- DSC Application Form
- Applicant ID Proof
- Authorization Letter by Organization Authorized Signatory
- Authorized Signatory Proof
- Proof of Organizational Existence

For issuance of SSL/TLS certificates, below verification shall be followed.

3.1. Domain Name Verification:

a. To demonstrate that the person requesting the certificate owns or controls the domain, each value provisioned for subject alternative names [DNS Names] must pass domain name verification.

b. This shall be accomplished by

I. Validating the request by communication to: webmaster@domainname.com, administrator@domainname.com,admin@domainname.com, hostmaster@domainname.com, postmaster@domainname.com, or any email ID listed in the technical, registrant, or administrative contact field of the domain's Registrar record; OR

II. Requiring a practical demonstration of domain control (Eg: making changes to DNS zone file or adding a unique file/filename on the domain under verification); This is achieved by CA sharing a unique Request Token or a Random Value, valid for a short duration, with the applicant and validating this data against the content of the file name provided or the DNS value (CNAME, TXT or CAA record) of the domain.

c. In the case of wildcard domains, these shall undergo additional checks, to as not to wrongly issue, for a domain listed in the public suffix list (PSL). If the domain is listed in PSL, the application shall be refused, unless the applicant proves ownership of the entire domain namespace.

d. In the case of IP Address, in place of the domain name, it shall be verified to have the applicant's control over the IP, using

(i) change in agreed information in an URL containing the IP address, OR
(ii) IP assignment document of IANA or Regional Internet Registry, OR
(iii)performing r-DNS lookup resulting in a domain name verified by the above procedure.

3.2. Organization Person verification

The verification of the identity & address of the applicant shall be carried out in the following manner

a. Identity of the applicant shall be verified by obtaining a legible copy of the employment ID and PAN card which noticeably shows the Applicant's face. The copy of the document shall be inspected for any indication of alteration or falsification. A video verification as per the procedure mentioned in Annexure VI shall be carried out by CA to ascertain the photo match of an applicant with the photo presented in the identity proof & DSC application form. The PAN number shall be electronically verified with the income tax database for matching the name as submitted in the DSC application form.

b. The applicant shall submit an authorization letter from the authorized signatory of the organization stating the authorization to apply for an SSL certificate. The letter shall contain the name, photo, designation, and address of the applicant. CA may ask for additional documents for the confirmation of the applicant's affiliation with an organization.

c. Additional verification may be made by the CA of the applicant's name & address for consistency with the website of the organization.
d. CA shall confirm that the applicant can receive communication via organizational telephone and email.

3.3. Organization Verification

- The organization verification includes authorization proof to the applicant and the existence of an organization.

- Sufficient document evidence shall be provided by the applicant for proof of authorized signatory

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

- The organization owns the domain name, or the organization is given the exclusive right and authority to use the domain name

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

- The documents/procedure required for proof of the existence the of organization are given in Annexure I.

b. Document Signer Certificate

This section specifies the verification requirements for issuance of Document Signer Certificate. The certificate profile requirements shall be as per the Interoperability Guidelines for Digital Signature Certificates (OCC-IOG). The Key generation requirements for the Document Signer Certificate shall be as per X.509 Certificate Policy for Nepal PKI(OCC-CP). The following direction is issued for strict compliance

- The applicant of Document Signer certificate shall be an organizational person of that organization. The verification requirements for Document Signer Certificate shall be as per section 2.3

- The following declarations shall be obtained from subscriber

- 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.

- I hereby declare that necessary controls have been built in software applications to ensure that there is no misuse
- I hereby declare and understand that the documents/messages authenticated using Organizational Document Signer Certificate issued to us is having organizational accountability.

****

Annexure I

Supporting documents for organization verification

Authorization to Authorized Signatories	
Category	**Documents required**
Individual/Proprietor ship Firm:	1.Business registration certificate containing name of the proprietor confirming the business ownership of Authorized signatory (Proprietor). 2.Government issued ID card (PAN, Voter ID, Passport or Driving 3.License) of Authorized signatory shall be enclosed.
Partnership Firm:	1.Copy of List of partners from Partnership Deed. (First page and page(s) containing Authorized Signatory/Partner Name) 2.If Authorized signatory is not a partner, an Authorization Letter signed by a partner. 3.Government issued ID card (PAN, Voter ID, Passport or Driving License) or organizational ID card of Authorized signatory shall be enclosed.
Corporate Entities:	1.Copy of List of Directors. CA shall cross verify such details in OCR Website. 2.If Authorized signatory is not a director, Board Resolution OR Power of Attorney shall be enclosed. 3.Government issued ID card (PAN, Voter ID, Passport or Driving License) or organizational ID card of Authorized signatory shall be enclosed
Association of person (body of individuals)	1.Copy of resolution from Association / Society authorizing the signatory. 2.Government issued ID card (PAN, Voter ID, Passport or Driving 3.License) or organizational ID card of Authorized signatory shall be enclosed.
Limited Liability Partnership	1.Copy of List of Directors. CA shall cross verify such details in OCR Website. 2.If Authorized signatory is not a director, Board Resolution OR Power of Attorney shall be enclosed. 3.Government issued ID card (PAN, Voter ID, Passport or Driving License) or organizational ID card of Authorized signatory shall be enclosed
Non-Government Organization /Trust	1.Copy of resolution from the NGO / Trust authorizing the signatory. 2.Government issued ID card (PAN, Voter ID, Passport or Driving License) or organizational ID card of Authorized signatory shall be enclosed
Banking Organization	1.Bank ID card of Authorized Signatory / Bank Manager

Government Organization	1.Copy of organizational ID card of Authorized signatory /identity letter issued by the organization/ Proof of individuals association with organization 2.letter of Authorized signatory to CA for eSign/DSC as per annexure V Authorized signatory shall meet the other requirements of Annexure V

Supporting Documents in respect of Existence of organization	
Category	**Documents required**
Individual/ Proprietorship Firm	The proof of organizational PAN verification details as mentioned in Annexure III. **OR all the below mentioned documents** Original Bank Statement with transactions less than 3 months, signed by the Bank. Bank Statement shall be in the "organization name". As an alternate to bank statement, a signed letter from the bank confirming the account existence and organization name can be provided. Copy of Organization Business registration certificate including Shops & Establishments
Partnership Firm	The proof of organizational VAT verification details as mentioned in Annexure III. **OR all the below mentioned documents** Original Bank Statement with transactions less than 3 months, signed by the Bank. Bank Statement shall be in the "organization name". As an alternate to bank statement, a signed letter from the bank confirming the account existence and organization name can be provided. Copy of Organization Business registration certificate including Shops & Establishments. Copy of Organization PAN Card
Corporate Entities	The proof of organizational VAT verification details as mentioned in Annexure III. **OR all the below mentioned documents** Original Bank Statement with transactions less than 3 months, signed by the Bank. Bank Statement shall be in the "organization name". As an alternate to bank statement, a signed letter from the bank confirming the account existence and organization name can be provided. Copy of Organization Incorporation Certificate. Copy of Organization PAN Card
Association of person (body of individuals)	The proof of organizational VAT verification details as mentioned in Annexure III. **OR all the below mentioned documents** Original Bank Statement with transactions less than 3 months, signed by the Bank. Bank Statement shall be in the "organization name". As an alternate to bank statement, a signed letter from the bank confirming

	the account existence and organization name can be provided. Copy of Organization Incorporation and Registration Certificate issued by authority such as Registrar. Copy of Organization PAN Card
Limited Liability Partnership	The proof of organizational VAT verification details as mentioned in Annexure III. **OR all the below mentioned documents** Original Bank Statement with transactions less than 3 months, signed by the Bank. Bank Statement shall be in the "organization name". As an alternate to bank statement, a signed letter from the bank confirming the account existence and organization name can be provided. Copy of Organization Incorporation certificate. Copy of Organization PAN Card
Non-Government Organization /Trust	Original Bank Statement with transactions less than 3 months, signed by the Bank. Bank Statement shall be in the "organization name". As an alternate to bank statement, a signed letter from the bank confirming the account existence and organization name can be provided. Copy of Organization Incorporation certificate. Copy of Organization PAN Card
Banking Organization	1) The proof of Bank VAT verification details as mentioned in Annexure III. **OR all the below mentioned documents** Copy of Bank PAN Card Copy of Incorporation Certificate or Banking License Certificate
Government Organization	As per Annexure V

Annexure II

Terms and conditions for use of HSM for class 3 Organizational Person DSCs

In the case of DSC (class 3) being applied for by Organizational 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 authorized signatory of the organization is enclosed assuring the following.

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

Annexure III

VAT registration Verification

1.	CA can use the organizational VAT details verification services provided by VAT office through APIs.
2.	The organizational details include Organization Name (Legal Name of the Organization), Address & status (active/non-active) at the time of verification.
3.	CA shall ensure the “organization name” is matching with the certificate application, and also ensure the organization is active with filings lesser than 3 months.
4.	CA shall preserve the digitally signed proof of organizational VAT details obtained from VAT services.
5.	The proof of verification shall be digitally signed by the CA.

Annexure IV

Document proof as Identity and address

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

Document as proof of identity (Any one):

- NID (eKYC Service)
- Passport
- Driving License
- PAN Card
- Post Office ID card
- Bank Account Passbook/statement containing the photograph and signed by an individual with attestation by the concerned Bank official.
- Photo ID card issued by the Ministry of Home Affairs of Centre/State Governments/Local Government.
- Any Government issued photo ID having Name & address.
-

Documents as proof of address (Any one):

- NID (eKYC Service)
- Telephone Bill
- Electricity Bill
- Water Bill
- Bank Statements signed by the bank
- VAT and Tax registration certificate.
- Driving License (DL)/ Registration certificate (RC)
- Voter ID Card
- Passport
- Property Tax/ Corporation/ Municipal Corporation Receipt
- Any Government issued photo ID having Name & address
-

With the above documents the following conditions will apply

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

2. ***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.

3. ***Digitally signed documents:*** For Digitally Signed photo id document by the issuer, it can be accepted in electronic format where CA can validate the Digital Signature. In such case, CA shall cross verify the photo with the video. The document shall be preserved along with its password (if any) for future references (Applicable for ePAN, Driving License etc being issued by respective issuers in digitally signed form)

Annexure V

The criteria for the eligibility of government organization and its authorized signatory

2.	Government organization includes Local/State/ Central Government and their departments, any agency/ instrumentality on which the Government has deep and pervasive control, PSUs, Government Companies, Government Corporations etc.
3.	For the government organizations, the authorized signatory shall be Controlling/Administrative Authority/Head of Office or Head of Department (HoD).
4.	For issuance of DSCs MPs having ID card, the approval of authorized signatory is not required during their tenure; however, their identity should be verified from the Local or state or central government websites. In the Local Government level, for issuance of DSC to elected members, the authorized signatory shall be the Chief Administrative Officer (CAO) for Chairman Or mayor whereas Chairman Or mayor will be authorized signatory for all other elected members and staffs.

5.	AUTHORIZED SIGNATORY LETTER TO CA FOR eSign/DSC (To be submitted to CA by Authorized Signatory) [APPLICABLE TO ALL CENTRAL GOVERNMENT EMPLOYEES, STATE GOVERNMENT EMPLOYEES, EMPLOYEES OF STATUTORY BODIES, PUBLIC SECTOR UNDERTAKINGS AND OTHER GOVERNMENT ORGANIZATIONS] To -----CA Name & Address------ I, Controlling / Administrative Authority / Head of Office / Head of Department (HoD) of the -- -----Organization Name ----------, have understood the requirements of eSign/DSC enrolments under provisions of Electronic Transaction Act, and will authorize the employees in line with these requirements. I have enclosed my ID card /identity letter issued by the organization/ Proof of association with the organization. Full Name: _____ Organization Name: _____ Position/Designation: _____ Organization Identity Card Number: _____ Office Address: _____ Office Tel No: _____ Mobile No:_____(Optional) Website Reference of my information, if any:_____(Optional)

	Signature:_____ (Seal & Stamp) Date: _____ Enclosed: ID card of Authorized signatory /identity letter issued by the organization/ Proof of individuals association with organization

Annexure VI

Video Verification

Video verification applies to DSC applicants, authorized signatories, and originals of the documents.

1.	CA shall make available a tamper proof video capture facility in their application.
2.	The video recording of interactive session with DSC applicant by using the facility provided by CA application shall be not less than 20 seconds.
3.	The video verification shall undergo at least two levels, one electronic and one manual level verification by CA. CA shall implement software capabilities to check face in video against photo obtained using KYC or eKYC to perform photo match for electronic verification.
4.	For manual check, trusted persons of CA shall perform verification for match of photo obtained through eKYC or KYC with the face in video.
5.	If automated video verification is not implemented, at least 2 trusted persons shall independently verify KYC data against video.
6.	CA shall not make available option for uploading offline video recording and also shall not accept offline recording by any other means.
7.	CA should allow only one-way video recording session with applicant.
8.	A traceable log of these capturing shall be clearly maintained, including the end user IP address (with date and time) used for capturing the video for individual and document verifications.
9.	In the video capturing, face should be fully visible, 50% of the video frame shall be covered by the face and background should be visible. Any video where face is not clearly visible, or at a far distance shall not be accepted. The face should have a bright light and there should not be dark shadows covering the face. The video of subscriber wearing any accessories like cap, headgear, eyeglasses, headphones and/or sun glasses shall not be accepted. Video should be preferably in a plain background and subscriber should have a natural expression. In the case of documents, during the capture, document should be preferably held using fingers on the edges without covering the contents of the document. Alternatively, document can be placed on a flat surface and recorded.
10.	The intention for applying for a DSC/eSign shall be expressed by the applicant during the video verification. Also, CA shall display at least three-digit random number and the reading of the same by applicant shall be captured & verified. CA shall implement the generation of fresh random number for each new video recording session. In case if the applicant is unable to speak due to dumbness or illness, the random number can be shown by the way of showing over fingers OR writing down and showing on paper. The sample format is as follows: *My name is hari subedi and I want to apply for a DSC/eSign through (CA name). The code is h34*
11.	CA shall carryout cross checking against earlier approved videos of the same applicant to avoid any duplication

12.	The video captures and the associated verification parameters in CA system shall be cryptographically timestamped using the timestamping service of CA within 6 hrs they are captured.
13.	Videos shall have a provable integrity check & prevent the reuse by implementing the mechanisms like visible watermarking/embossing with date-time on the video etc.

****

4. Guidelines for e-authentication using NID e-KYC services

In accordance with the Electronic Transaction Act, Certifying Authorities (CA) are responsible for issuing Digital Signature Certificates (DSC) after successfully verifying the applicant's address and identity. These rules are meant to be applied when CAs issue DSCs DSC applicants who have NID numbers and email addresses or mobile phone numbers that are registered in the NIDMC Database. After verifying a DSC applicant's finger print, CA facilitate a pass code authentication mechanism through the application interface if their email address and mobile phone number are not already listed in the NIDMC Database. The NID eKYC service's biometric authentication must be used by CAs to generate DSC This mechanism can be used as a challenge password for subsequent authentication steps. application forms for DSC applicants part of.

a) Applicant's email or mobile numbers are pre-requisites for issuance of Digital Signature Certificate through NID e-KYC verification channel.

b) CA should be an authorized e-KYC user agency of National ID Department of Nepal (NIDMC).

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 subscriber's NID number should be used to construct the DSC application form, which should then be filled up with the data from NIDMC and signed by the DSC applicant. Online confirmation should be done for further information such as PAN, DSC class, etc.

f) NIDMC offers digitally signed information about DSC applicant using NID e-KYC service. Name, address, email address, cell phone number, photo, and response code are all included. The answer code, which NIDMC keeps offline for an additional two years and online for six months, should be noted on the application form and added to the DSC. In accordance with the standards outlined in the Electronic Transaction Act, CAs should maintain the digitally signed verification information.

g) Any additional information that must be included in the digital signature certificate but is not a part of the information obtained from NIDMC, such as PAN, etc., must be confirmed by the CA, and the documentation of that verification must be kept

h) In the case of organizational person certificates, the name, photo, and response code details obtained from NID eKYC services must be automatically fileed out on the DSC application form, Fill out the remaining fields in accordance with organization's person verification requirements.