IDENTITY VERIFICATION GUIDELINES

Version 2.3

15.02.2023

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	IDENTITY VERIFICATION GUIDELINES
Status	Release
Version	2.3
Release Date	15.02.2023
Last update	15.02.2023
Document Owner	Controller of Certifying Authorities, India

Contents

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 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.

“Registration Authority” or “RA” is an entity engaged by CA to facilitate the submission of applicant’s credentials to CA for the eKYC account creation

1 Guidelines to CAs

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. The guidelines issued by the Controller of Certifying Authorities are to be strictly followed by CAs .

1.1 General	
1.	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 shall be referred to or incorporated in the subsequent revision of CPS of CAs.
2.	CA shall make sure the following text shall be displayed to the user before submission / signing 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.*
3.	The eKYC information collected from applicant shall not be shared by CA and comply with all the provisions of IT Act for protecting the information specifically Rule 33 and 34 of IT CA Rules
4.	The subscriber's registered information with CA such as video, photo, ID cards, phone number, PAN/Aadhaar, other information submitted and not a part of certificate in readable form are 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 IT Act, shall be liable for penalty for breach of confidentiality and privacy under section 72 of IT Act.
1.2 eKYC Account	
1.	eKYC account of DSC applicant is mandatory for applying for a DSC or availing eSign service. The verified information held by CA shall be used for issuance of DSC or eSign. For eSign service based on online Aadhaar authentication, eKYC account is not required
2.	The eKYC account of the DSC applicant shall be created by CA based on eKYC of applicant (Bank, Organisational, PAN and Offline/Online Aadhaar) or a direct verification (Foreign Nationals) . The information which are required in DSC application form and not present in the eKYC of applicant shall be submitted by the eKYC applicant and verified by CA before activating the eKYC account.
3.	In case eKYC account holder requires more than one account (fore.g personal and organizational), eKYC account holder must undergo all the verification procedures mentioned for the additional eKYC option. CA should treat both eKYC accounts logically under one eKYC account of the eKYC applicant. The mobile number and PAN can be the same. For user authentication, CA shall provide an option for selecting the account mode (personal/organizational)
4.	The validity of eKYC account shall not be more than 2 years. The account (with same

	username, PAN, Mobile) can be extended only through carrying a fresh verification of the applicant under these guidelines.
5.	In case CA is not able to ascertain the genuineness of the e-KYC data submitted by applicant, CA shall reject the request
6.	CA shall notify applicant the subscriber agreement for the use of KYC information for DSC issuance by CA on successful authentication by the applicant. The applicant shall have option to accept or reject the same.
7.	Applicant shall 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.
8.	Applicant shall have an option to activate, deactivate and close account at any point.
9.	Appropriate fraud detection and preventive security mechanisms shall be implemented against enrollment frauds. Specifically CA should make sure that the page capturing PIN shall be free from the threat like phishing attacks, malicious plug-in, hijack clicks/key strokes etc
10.	CA shall have approval of CCA for maintaining eKYC account for applicants.
11.	The format of the eKYC account ID shall be of the format: id@id-type.esp-id. The allowed eKYC account id type are username, Mobile are PAN. The PIN shall be created along with eKYC account ID. eKYC account user ID change is not allowed after creation.
12.	The PIN reset shall be with mobile OTP and email verification. In the absence of email, it shall be mobile OTP and video verification. In the case of banking where email is not captured earlier, the PIN reset shall be allowed only after successful matching of fresh eKYC with the registered eKYC details.
1.3 DSC Application Form	
1.	DSC application form shall be generated by CA based on the verified information held in eKYC account maintained by CA after obtaining the two-factor authentication of the applicant.
2.	The electronic signature of the applicant in the DSC application form shall be affixed using the eSign service of the CA.
3.	Power of attorney is not allowed for the purpose of DSC application to CA and Issuance of DSC.
4.	A CA may ask for more supporting documents, if they are not satisfied with the documents that have been submitted.
1.4 Mandatory Information in the DSC application Form	
1.	Name, address (residence/organisation), email, Mobile Number, PAN/Aadhaar no (Last four digit), Photo, Date, type certificate (personal/organisational), signature of applicant and Class are mandatory in the eKYC account and DSC application form for issuance of DSC. Email is optional for eKYC account to be created only for the purpose of eSign.
2.	For all categories of DSC applicants, it is mandatory to provide either PAN or Aadhaar Number.

1.5 Name	
1.	The name of the DSC applicant shall be same as the name in respective eKYC
2.	For proof of Identity, copy of at least one photo Identity proof bearing name of the applicant , as mentioned in the Annexure IV , shall be submitted
1.6 Address	
1.	The address of the DSC applicant shall be residential or organisational.
2.	For address proof, the applicable list of documents are given in Annexure IV
1.7 Mobile Number	
1.	Mobile Number of applicant is a pre-requisite for creation of eKYC account by CA for applicant.
2.	For the proof possession of mobile number, CA shall send a SMS OTP and the same shall be verified by capturing through the interface provided by CA. 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 the compromise.
1.8 Email address	
1.	Email id of the applicant is mandatory for issuance of DSC based on the eKYC account activated by CA. Email id is optional for the eKYC accounts activated only for the purpose of eSign.
2.	CAs shall put in measures to ensure that email addresses that are included in Digital Signature Certificates (DSC) are unique to the DSC applicant.
3.	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 same DSC applicant.
4.	For email verification, CA shall send an email OTP or challenge response or verification URL to the email of DSC applicant and verify 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.
5.	No disposable email (fast temporary email without registration) shall be accepted by CA.
1.9 PAN	
1.	CA shall electronically verify the PAN number with Income tax database through eKYC service and accept only if the name is matching correctly. CA shall preserve the proof of verification with their digital signature
1.10 Verification	
1.	Verification is the electronic verification of the identity and information submitted by eKYC applicant for the purpose of creating an eKYC account with CA for eSign or DSC issuance.
2.	The verification requirements may vary depending on the source of eKYC like Aadhaar, Bank or organisation.
3.	CA shall allow only the automatic population of digitally signed information received from source of eKYC like Aadhaar or Bank in the electronic application form. The information received from the other source (like PAN and GSTN) shall be used only for cross verifying the information submitted by the applicant in the interface

	provided by CA.
1.11 Physical verification/Video verification/ on-line Aadhaar eKYC	
1.	The physical verification of DSC applicant shall be carried out using online interactive video verification directly by CA as per Annexure VI or by online Aadhaar eKYC Biometric Authentication
2.	Irrespective of the initial mode of in-person verification, in the subsequent verification, CA shall carry out photo match of applicant with that in CA eKYC records.
3.	CA shall check any indication of alteration or falsification in video recording
1.12 Documents verification	
1.	In lieu of the attestation of documents exists in the paper-based DSC application; 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 source of issuance of the documents.
2.	If applicable, the originals of the identity and address proof shall be verified during the video verification.
3.	The video verification of the original documents shall be carried out as per Annexure VI
4.	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	
1.	CA shall issue class 3 level individual signing certificate (both Personal & organizational) to the private key generated on a FIPS 140-2 level 2/3 validated Hardware cryptographic module (crypto tokens) with both Class 2 and Class 3 OID in the policy field. CA shall not issue class 2 level individual Signing certificates alone instead CA shall issue Class 3 individual signing certificates with a combination of both class 2 & class 3 certificates by including Class 2 OID in the Class 3 certificates. Class 3 individual signing certificates shall be qualified as both class 2 & class 3 individual signing certificates.
2.	CA shall put procedure in place to ensure that no Class 3 individual Signing DSCs are issued in cases where the key pair has not been generated on a FIPS 140-2 level 2/3 validated Hardware cryptographic module (crypto tokens).
3.	For protection of crypto token against “PIN reset compromise”, a) CA shall not support PIN reset procedure for subscriber’s crypto token, unless the crypto token is re-initialized / formatted. For the convenience of DSC applicant on such scenarios, CA shall re-issue the certificate for the remaining period of validity of the certificate. Such re-issuance shall be provided free of cost, at least once per certificate. CA may provide additional re-issuance which may be charged extra by CA to the user. CA shall carryout such re-issuance only after authentication of the subscriber. b) From 01.04.2023 onwards, CA shall not allow the download of DSC to crypto token having default password.
4.	A list of approved cryptographic device manufacturers / suppliers and information relating to their FIPS 140-2 Level 2/3 validated tokens must be published on the

	website of the CA.
5.	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.
6.	Terms and conditions for use of HSM for class 3 Organisational Person DSCs on FIPS 140-2 level 2/3 certified HSMs shall be as per annexure II.
1.14 Invoice/Acknowledgement	
1.	In the case of Personal/Organisational Person Digital Signature Certificate issuance (Class 1, Class 2 and Class 3), CA shall provide direct invoice/acknowledgement of DSC issuance to the DSC applicant or applicant's organisation. CA shall carry out periodic reconciliation of invoice/acknowledgement with corresponding DSC issued to subscriber. Copy of the invoice/acknowledgement issued to DSC applicant shall be preserved by CA.
1.15 Subscriber Agreement	
1.	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.
2.	For eKYC account creation based on the KYC information source such as Offline Aadhaar KYC, Banking and organisational , the eSign of the subscriber shall be based on the information received from the KYC information source.
1.16 DSC Issuance	
1.	DSC shall be issued only up on satisfying the verification requirements specified in the respective eKYC sections in this document. The maximum time limit for the download of DSC shall be 30 days from the date of completion of verification/approval. If the download of DSC is not carried out by the applicant within 30 days, applicable verification requirements specified in the respective eKYC sections in this document shall be carried out by CA before DSC issuance
1.17 Archival	
1.	CAs shall preserve the digitally signed documents, proof of verification information, logs etc. as per the requirements mentioned in the Information Technology Act.
2.	Archival of information shall be 7 years from the date of expiry of the Digital Signature Certificate.
1.18 Role of Trusted person	
1.	CA shall make sure that the CA Verification Officer's roles and responsibilities are not be delegated or controlled by anyone else.
2.	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.
3.	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	
1.	Apart from the details required for creation of eKYC account, the additional details

	shall be verified by CA in accordance with the type of special purpose certificate.
2.	Only organisational persons are allowed to apply for special purpose certificate.
3.	CA shall verify all the information to be 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	
1.	For encryption certificates, CA shall provide key escrow facility, where key pair is securely stored and managed by CA. The key shall be retrievable again by the DSC applicant at any point of time, even after expiry of the certificate. This shall be retained by CA for minimum of 7 years from the expiry of the certificate. CA shall allow the download of the escrowed key only after a successful video verification of the applicant.
2.	The encryption keys and certificates shall be preserved by subscriber also.
1.21 First factor Authentication	
1.	The first factor authentication to eKYC account shall be PIN
1.22 Second factor Authentication	
1.	The second factor authentication can be SMS-OTP or the other authentication mode specified in the eSign API
2.	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	
1.	CA shall always send OTP to eKYC account holder with PURPOSE relevant to the authentication seeking for. OTP should be a newly generated random number for each transaction.
2.	OTP shall be sent only to the verified mobile number registered in the eKYC account.
1.24 Registration Authorities (RAs)	
1.	Role of RA is strictly restricted to facilitate the submission of details to CAs for eKYC account creation/DSC issuance process of DSC applicant.
2.	CA shall carryout KYC in line with Organization KYC option of Identity Verification Guidelines and create an eKYC account for RAs. The eKYC account shall be created after the verification of Name, Address, email, mobile no, PAN, proof of existence of RA, GST (in case applicable) and video/Aadhaar bio-metric based verification.
3.	CA shall not have any direct interface to RA for eKYC account process/DSC issuance process of DSC applicant however restricted monitoring facility can be provided till the approval of DSC application by CA, such monitoring facility shall be restricted only to the single RA who facilitated DSC application form submission.
4.	RAs access to CA system shall be based on two factor authentication.
5.	CA shall have an electronically signed agreement (eSign service) with RAs which shall include the following 1. RA shall protect the confidentiality of DSC applicant's information or data. 2. RA shall not download, store, make copies, captures, publishes, transmits or extracts any data or information pertain to DSC applicant.

	3. RA shall restrict agreement related issues with CA or with law and enforcement agencies only. 4. Any impersonation or any assistance in this regard / misrepresentation or suppresses any material fact or any assistance in this regard/ dishonest /fraudulent actions of RA shall be liable for the termination of agreement with CA and legal action. 5. Any communication, for the purpose of causing annoyance, inconvenience, obstruction, enmity and ill will to CA, on the matter related to agreement between CA and RA, to the external agencies shall be liable for the termination of agreement with CA 6. RA shall protect their computer hardware, software, and procedures that are secure from intrusion and misuse 7. CA shall have right to Audit the RA to check the compliance of the agreement and reserve right to terminate agreement in case of any non-compliance.
6.	CA may register a complaint against RA with law and enforcement agencies for assistance in misrepresentation or suppresses any material fact or any violation of this section 1.24
7.	CA shall carryout Audit of RAs to check the compliance of the agreement, on sample basis based on need or in the case of any anomalies and such audit report shall be made available to CA auditors for inspection.
1.25 Additional Physical Verification	
1.	The additional physical verification of DSC applicant is optional, however if opted the OID 2.16.356.100.10.2 shall be mentioned in the policy id field of certificate.
2.	For highest level of assurance, in addition to all the requirements mentioned in this document, an authorised person employed by the CA shall verify the physical presence of DSC applicant and also verify the genuineness of all the documents submitted.
3.	The authorised person employed by the CA shall also verify the possession and proof of registration of the mobile number, address proof, identity, ink signature verification, neighbourhood enquiry etc. or any additional requirements to eliminate the possibility of impersonation.

2 Guidelines for maintaining 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	
1.	CA to verify the applicant one time and issue DSC subsequently based on 2-factor authentication by applicant. The two factor authentication includes the PIN set by the applicant and a second factor, as permitted by the guidelines issued by CCA. (Eg: OTP sent to the verified mobile).
2.	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 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 shall keep user name limited to few characters. d) CA shall ensure username is unique within their system. For Personal eKYC accounts, the mobile number and PAN shall be unique.
2.2	**Aadhaar eKYC**
1.	These guidelines are intended to be used to create eKYC account who have Aadhaar Number registered in UIDAI Database.
2.	CAs are required to follow the requirements specified by UIDAI strictly for eKYC authentication of DSC applicant
3.	As part of the e-KYC process prescribed by UIDAI under Aadhaar Act, the applicant for DSC authorizes CA (through Aadhaar eKYC) to obtain their demographic data along with his/her photograph (digitally signed and encrypted) to CAs for verification.
2.2.1	**Aadhaar online eKYC**
1.	This section is allowed as per the OM(File No. 13(6)/2018-EG-II(Pt)), dated 18 Jan 2022 , to use Aadhaar e-KYC authentication by Certifying Authorities under the CCA for issue of Digital Signature Certificate (DSC) under Section 3A of the IT Act along with the e-signature also in compliance with Section 4(4)(b)(i) of the Aadhaar Act, 2016 as amended.
2.	CA shall be an authorized e-KYC User Agency (KUA) of Unique Identification Authority of India (UIDAI).
3.	CA shall provide direct interface for capturing information required for e-KYC services of UIDAI
4.	Subscriber shall submit Aadhaar Number and perform Biometric/OTP eKYC authentication to UIDAI through the interface provided by CA only.
5.	Up on receipt of Aadhaar eKYC XML from UIDAI, CA decrypts, validates UIDAI signature, reads and extracts demographic data, and photo.
6.	The verified information received through online Aadhaar e-KYC shall be used for creation eKYC account of user.
7.	The DSC application form should be generated by populating the information received from UIDAI.
8.	The application should be signed by DSC applicant. The verified information received through e-KYC services can be used for obtaining eSign of DSC applicant by CA through a separate user eKYC authentication.
9.	If PAN of the applicant is to be included in eKYC account for embedding it in the certificate, CA shall verify the same prior to inclusion in the eKYC account.
10.	On successful Aadhaar eKYC Authentication for the eKYC Account, CA shall store the unique UID Token for that Aadhaar holder against such eKYC Account. This shall be used for referring to same user during any re-verification requirements.
11.	For DSC issuance, email shall be included in the eKYC account after verification by CA.
12.	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.

2.2.1.1 Aadhaar online eKYC – OTP	
1.	Subscriber submits Aadhaar Number and performs provides OTP authentication through the interface provided by CA to UIDAI.
2.	Up on Successful authentication, CA receive Aadhaar e-KYC XML and create e-KYC account for the applicant.
3.	The mobile number is mandatory. CA shall capture the mobile number of the user and carryout verification of Mobile Number.
4.	CA does interactive video verification (Annexure VI) and also does a photo match of Aadhaar eKYC photo with the video.
5.	For each DSC issuance, video verification shall have been carried out within last 2 days. The in-person verification can also be substituted by Aadhaar Biometric Authentication.
2.2.1.2 Aadhaar online eKYC – Biometric	
1.	Subscriber submits Aadhaar Number and performs biometric authentication through the interface provided by CA to UIDAI.
2.	Up on successful authentication, CA receives Aadhaar e-KYC XML and creates e-KYC account for applicant.
3.	The mobile number is mandatory. CA shall capture the mobile number of the applicant and carryout verification of Mobile Number.
4.	For each DSC issuance, Aadhaar eKYC Biometric authentication of applicant shall have carried out within last 2 days and CA should accept only if the face in Aadhaar Photo matches against that in CA eKYC record of same applicant. The in-person verification can also be substituted by interactive video verification (Annexure VI) provided that CA should successfully verifies the matching face in video with the photograph of eKYC record of the same applicant.
2.2.2 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 shall accept the mobile number within offline KYC only, no changes are allowed.
5.	For issuance of DSC, CA captures email for communications, alerts, and PIN reset options and it must be verified.
6.	If PAN of the applicant is to be included in eKYC account for embedding it into the certificate, CA shall 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 (Annexure VI) and also does a photo match of Aadhaar eKYC photo with the video.
9.	For each DSC issuance, video verification shall have carried out within last 2 days. The in-person verification can also be substituted by Aadhaar eKYC Biometric Authentication provided that CA successfully verifies the face in Aadhaar Photo against that in KYC record.
10.	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.
2.3 Organisational KYC for Organisational Person Certificates	
This section is applicable for eKYC applicant affiliated to organizations	
1.	For organisational person certificate, the Organization Name (O Value) in the certificate shall

	match the organization name and also in compliance with naming convention specified CCA-IOG.
2.	The minimum requirements for Issuance of DSC to organisation person include: a) eKYC account of Applicant b) Applicant ID Proof or Proof of individuals association with organisation c) Letter of Authorization by Organization to Authorized Signatory for self authorisation and also to other DSC applicants. d) eKYC account of Authorized Signatory and authorization to DSC applicant e) Proof of existence of organization
3.	CA shall carry out the verification of the existence of organization & authorised signatory of the organization as per 2.3.1. All the information submitted by eKYC applicant for eKYC account shall be digitally signed by authorised signatory.
4.	The criteria for the eligibility of government organisation and its authorised signatory are given in the annexure V.
5.	KYC of organisational eKYC applicant shall be submitted to CA and CA carryout the verification.
6.	The eKYC account request shall include Name, Office address, photo, PAN, mobile no, Organisational ID, email etc. The mobile number and PAN of the applicants are mandatory. The copy of the organisational ID card and PAN shall also be submitted to CA.
7.	CA shall carry out interactive video verification as per Annexure VI and shall verify the photo match of eKYC photo with the video. The original document verification is also a part of video verification. The in-person verification can also be substituted by Aadhaar eKYC Biometric Authentication provided that CA successfully verifies the face in Aadhaar Photo against that in KYC record.
8.	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 eKYC applicant.
9.	CA shall provide Organizational eKYC applicant to set up PIN and user ID upon the authentication by CA.
10.	In case of any change in account holder's status or information, the request for change shall be submitted with the authorization of authorised signatory.
11.	CA shall accept the mobile number within Organisational KYC only, no changes are allowed.
12.	For DSC issuance, the video verification shall have carried out within last 2 days
2.3.1	**Verification of Authorised Signatory**
1.	The scanned copy of the documents for 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.
2.	The steps 4-7 of 2.3 shall be followed for the verification prior to the eKYC account creation.
3.	CA shall carryout secondary verification like face-to-face interaction/web site reference/call to organizational telephone numbers to confirm the organizational identity of authorised person and the proof of the verification shall be maintained.
4.	The steps 8-9 of 2.3 shall be applicable for the eKYC account creation.
5.	Upon successful confirmation of organizational identity of authorised person, CA shall create an eKYC account and may issue DSC to authorised signatory. The DSC/eKYC Account of the

	authorized signatory shall be registered with CA and shall be mapped with the name of the verified organisation. Subsequently all the information submitted by eKYC applicant for eKYC account shall be digitally signed by authorised signatory. The DSC of the authorised signatory shall be asserted with OID 2.16.356.100.10.3 in the policy id field along with policy id for class of certificate
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 Information is verified in MCA website. In case of proprietorship organization where applicant himself/herself is the proprietorship, self-authorization / no authorization is required.
2.4	**Banking eKYC for Banking Customers**
1.	This section is applicable only for persons having 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.
2.	CA shall verify the source of the request and signature of bank prior to accept KYC information
3.	CA shall have an agreement/undertaking with Bank.
4.	CA shall carry out verification of existence of Bank, authorised signatory's identity as mentioned in Annexure I of the Identity Verification guidelines
5.	The DSC to be used for signature by bank shall be registered with CA and shall be mapped with the bank ID/Name
6.	The KYC details shall include Name, address, photo, PAN/Aadhaar Number, mobile no, Bank account No, Bank IFSC code (if applicable).
7.	The mobile number and PAN/Aadhaar Number(last four digit) of the applicants are mandatory
8.	CA shall allow eKYC applicant to set up PIN and user ID up on the authentication by CA.
9.	CA activates eKYC account after mobile verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with 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 KYC of the account holder from the Bank within last 24 hours.
2.5	**PAN eKYC for Personal Certificates**
1.	This section is applicable only for persons who submit the PAN & other KYC information to CA directly.
2.	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
3.	CA shall carryout verification of Mobile Number and PAN (eKYC). Email shall be captured and verified for DSC issuance.
4.	The video verification of the applicant shall be carried out by CA as per Annexure VI. During the video verification, the applicant shall display original PAN card and Government ID having 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.
5.	CA shall electronically verify the PAN number with Income tax database through eKYC service and accept only if the name is matching correctly. The digitally signed proof of the verified

	response shall be preserved by CA.
6.	CA shall verify the Government ID having address submitted to CA against the original displayed during the video verification.
7.	The eKYC account request shall include Name (as in PAN), residential address (as in address id), photo, PAN, mobile no, email etc.
8.	CA activates 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.
9.	In case of any change in account holder's information after activation of account, CA shall carry out fresh enrollment.
10.	CA shall allow eKYC applicant to set up PIN and user ID up on the authentication by CA.
11.	For DSC issuance, video verification shall have carried out within last 2 days. The in-person verification can also be substituted by Aadhaar eKYC Biometric Authentication provided that CA successfully verifies the face in Aadhaar Photo against that in KYC record.
2.6	**eKYC for foreign applicants**
1.	This section is applicable only for foreign applicants who submit the KYC information to CA directly. An 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.
2.	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.
3.	For organisational person certificate, a) Scanned copy of organisational id, organisational email id, mobile number, organisational address and letter of authorization from organisation are required. b) For the proof of organisational existence, publically verifiable and listed/recognized by local government reference of organisation in database/registry shall be provided. c) If the organisation is already registered/empanelled in government organizations of India, then the scanned copy of the letter of request issued from Indian government organisation with the details of DSC applicant can be accepted as address proof/existence of organisation for DSC issuance.
4.	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 embassy with residential address can be provided
5.	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.
6.	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
7.	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.
8.	In case of any change in account holder's information after activation of account, CA shall carry out a fresh enrollment.
9.	CA shall allow eKYC applicant to set up PIN and user ID up on the authentication by CA. The OTP can be sent to email of eKYC user.
10.	During the validity period of eKYC account, a fresh video verification shall have carried out for each DSC issuance within last 2 days.
11.	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 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 shall have standalone certificate issuance system for SSL issuance and CAs public key has been certified under special purpose root hierarchy. eKYC account of applicant is mandatory .

3.1 SSL Certificates

The issuances of SSL certificates by Licensed CAs are limited only to .IN domain. Only organisational 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 with necessary supporting documents. The minimum set of documents to be submitted includes:

1. DSC Application Form
2. Applicant ID Proof
3. Authorization Letter by Organization Authorized Signatory
4. Authorized Signatory Proof
5. Proof of Organizational Existence

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

1. Domain Name Verification:	
a.	Each value provisioned for subject alternative names (dnsNames) shall undergo domain name verification to prove the ownership / control of the domain by the requestor of the certificate.
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 case of wildcard domains, these shall undergo additional checks, to not to wrongly issue, for a domain listed in public suffix list (PSL). If the domain is listed in PSL, the application shall be refused, unless applicant proves ownership of entire domain namespace.
d.	In case of IP Address, in place of domain name, it shall be verified to have the applicant's control over the IP, by means of (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 above procedure.
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 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 applicant with the photo presented in the identity proof & DSC application form. The PAN number shall be electronically verified with income tax database for matching of 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 SSL certificate. The letter shall contain name, photo, designation and address of the applicant. CA may ask additional documents for the confirmation of applicant's affiliation to organization.
c.	Additional verification may be made by the CA the applicant's name & address for consistency with a website of the organization.
d.	CA shall confirm that the applicant is able to receive communication to organisational telephone and email.
3. Organization Verification	
1.	The organization verification includes authorization proof to applicant and existence of organization.
2.	Sufficient document evidence shall be provided by the applicant for proof of authorized signatory.
3.	Apart from the organizational person verification, the additional process documentation and authentication requirements for SSL certificate shall include the following: o The organization owns the domain name, or the organization is given the exclusive right and authority to use the domain name o 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)
4.	The documents/procedure required for proof of existence of organization are given in annexure I.

3.2 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 (CCA-IOG). The Key generation requirements for the Document Signer Certificate shall be as per X.509 Certificate Policy for India PKI(CCA-CP). The following direction is issued for strict compliance:

1.	The applicant of Document Signer certificate shall be an organisational person of that organisation. The verification requirements for Document Signer Certificate shall be as per section 2.3
2.	The following declarations shall be obtained from subscriber 1. 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. 2. I hereby declare that necessary controls have been built in software applications to ensure that there is no misuse 3. I hereby declare and understand that the documents/messages authenticated using Organisational Document Signer Certificate issued to us is having organisational accountability.

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

Under the Information Technology Act, Digital Signature Certificates (DSC) are being issued by Certifying Authorities (CA) on successful verification of the identity and address credentials of the applicant. These guidelines are intended to be used to issue DSCs by CAs to DSC applicants who have Aadhaar Number with the email-Id or mobile phone number registered in UIDAI Database. In case email-Id and mobile phone number is not registered in UIDAI Database, CA can facilitate a pass code authentication mechanism for DSC applicant through application interface after finger print verification, which can be used as challenge password for further authentication process. CAs needs to provide a mechanism to generate DSC application form for DSC applicant based on the biometric authentication through Aadhaar eKYC service. As part of the e-KYC process, the applicant for DSC authorizes UIDAI (through Aadhaar authentication using biometric) to provide their demographic data along with his/her photograph (digitally signed and encrypted) to CAs for verification. The DSC applicant's information received by CAs using Aadhaar eKYC service should be preserved by CA.

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

Annexure I - Supporting documents for organisation verification

Authorization to Authorized Signatories	
Category	**Documents required**
Individual/Proprietorship 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 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 MCA 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 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 MCA 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 Organisation /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 organisation 2. letter of Authorized signatory to CA for eSign/DSC as per annexure V

	3. Authorized signatory shall meet the other requirements of Annexure V

Supporting Documents in respect of Existence of organization	
Category	**Documents required**
Individual/Proprietorship Firm	1) The proof of organisational GST verification details as mentioned in Annexure III. **OR all the below mentioned documents** 1) 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 organisation name can be provided. 2) Copy of Organization Business registration certificate including Shops & Establishments
Partnership Firm	1) The proof of organisational GST verification details as mentioned in Annexure III. **OR all the below mentioned documents** 1) 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 organisation name can be provided. 2) Copy of Organization Business registration certificate including Shops & Establishments. 3) Copy of Organization PAN Card
Corporate Entities	The proof of organisational GST verification details as mentioned in Annexure III. **OR all the below mentioned documents** 1) 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 organisation name can be provided. 2) Copy of Organization Incorporation Certificate. 3) Copy of Organization PAN Card
Association of person (body of individuals)	1) The proof of organisational GST verification details as mentioned in Annexure III. **OR all the below mentioned documents** 1) 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 organisation name can be provided. 2) Copy of Organization Incorporation and Registration Certificate issued by authority such as Registrar. 3) Copy of Organization PAN Card
Limited Liability Partnership	1) The proof of organisational GST verification details as mentioned in Annexure III. **OR all the below mentioned documents** 1) 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 organisation name can be provided. 2) Copy of Organization Incorporation certificate. 3) Copy of Organization PAN Card
Non-Government Organisation /Trust	1) 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 organisation name can be provided. 2) Copy of Organization Incorporation certificate. 3) Copy of Organization PAN Card
Banking Organization	1) The proof of Bank GST verification details as mentioned in Annexure III. **OR all the below mentioned documents** 1) Copy of Bank PAN Card 2) 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 Organisational Person DSCs

In the case of DSC (class 3) being applied for by Organisational Person, if the key-pairs are proposed to be generated on Hardware Security Module (FIPS 140-2 level 2/3 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.

1.	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).
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 (Organisation Name).
5.	The following are the details of the HSM being used: • make, • model • unique identification number(s)

Annexure III - GST registration Verification

1.	For GST verification, CA shall be ASP/GSP of GST-GSP where GSP application expose GST System functionalities to ASP/GSP
2.	CA shall use only the organisational GST details verification services provided by GST or their approved GSPs through APIs
3.	The organisational details include Organisation Name (Legal Name of the Organization), Address & status (active/non-active) at the time of verification.
4.	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.
5.	CA shall preserve the digitally signed proof of organisational GST details obtained from GST services.
6.	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):

1. Aadhaar (eKYC Service)
2. Passport
3. Driving License
4. PAN Card
5. Post Office ID card
6. Bank Account Passbook/statement containing the photograph and signed by an individual with attestation by the concerned Bank official.
7. Photo ID card issued by the Ministry of Home Affairs of Centre/State Governments.
8. Any Government issued photo ID having Name & address.

Documents as proof of address (Any one):

1. Aadhaar (eKYC Service)
2. Telephone Bill
3. Electricity Bill
4. Water Bill
5. Gas connection
6. Bank Statements signed by the bank
7. Service Tax/VAT Tax/Sales Tax registration certificate.
8. Driving License (DL)/ Registration certificate (RC)
9. Voter ID Card
10. Passport
11. Property Tax/ Corporation/ Municipal Corporation Receipt
12. 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, gas, 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 organisation and its authorised signatory

1.	As per Article 12 in The Constitution Of India 1949, 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
2.	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.
3.	For the government organizations, the authorised signatory shall be Controlling/Administrative Authority/Head of Office or Head of Department (HoD).
4.	For issuance of DSCs MPs and MLAs having ID card, the approval of authorised signatory is not required during their tenure; however their identity should be verified from the state or central government websites. In the panchayat level, for issuance of DSC to elected members, the authorised signatory shall be the Block Development Officer (BDO).
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 Information Technology 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 is applicable to DSC applicants, authorised 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 Pankaj srivatstava and I want to apply for a DSC/eSign through (CA name) . The code is X22*
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.

****

Change History

1. Date 15.02.2023 (Deletions- ~~strikethrough~~, additions -underlined)

1.13 Key Pair Generation/Storage	
7.	For protection of crypto token against "PIN reset compromise", ~~CA shall follow any of the following options.-~~ c) CA shall not support PIN reset procedure for subscriber's crypto token, unless the crypto token is re-initialized / formatted. For the convenience of DSC applicant on such scenarios, CA shall re-issue the certificate for the remaining period of validity of the certificate. Such re-issuance shall be provided free of cost, at least once per certificate. CA may provide additional re-issuance which may be charged extra by CA to the user. CA shall carryout such re-issuance only after authentication of the subscriber. d) ~~For encryption certificate, The resetting password of 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 applicant in respect of crypto token management software/upgrading firmware/resetting passwords etc and CA shall complete the migration to this mode latest by December 31st 2021.~~ e) From 01.04.2023 onwards, CA shall not allow the download of DSC to crypto token having default password.
1.18 Registration Authorities (RAs)	
3	CA shall not have any direct interface to RA for eKYC account process/DSC issuance process of DSC applicant however restricted monitoring facility can be provided till the approval of DSC application by CA, such monitoring facility shall be restricted only to the single RA who facilitated DSC application form submission.
1.23 SMS-OTP	
1.	CA shall always send OTP to eKYC account holder with PURPOSE relevant to the authentication seeking for. OTP should be a newly generated random number for each transaction.
1.25 Additional Physical Verification	
1.	The additional physical verification of DSC applicant is optional, however if opted the OID 2.16.356.100.10.2 shall be mentioned in the policy id field of certificate.
2.	For highest level of assurance, in addition to all the requirements mentioned in this document, an authorised person employed by the CA shall verify the physical presence of DSC applicant and also verify the genuineness of all the documents submitted.
3.	The authorised person employed by the CA shall also verify the possession and proof of registration of the mobile number, address proof, identity, ink signature verification, neighbourhood enquiry etc. or any additional requirements to eliminate the possibility of impersonation.