CA FUNCTIONAL TESTING AND VERIFICATION

Version1.0

31 MAY 2024

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Table of Contents

1. Introduction

The CCA has issued multiple guidelines over a period of time to standardize the security and compliance requisites followed by CAs. Additionally, various guidelines have been published internationally intended to strengthen the security of the CA systems have been included in the guidelines for CA systems under RCAI. This documents describes integrated set of functional testing requirements necessary (but not limited to) for the application, OS, network and Certificates.

CCA mandates all CAs to get their operations audited annually by an empaneled auditor and the functional testing to be carried out by Cert-In empanelled agencies . . This document details the controls and the corresponding checks which need to be implemented for ensuring secure CA systems.

2. *Detailed Functional Testing/Verification of Controls*

2.1 Identity Verification Guidelines(CCA-IVG)

Control No.	Controls	Functional Test/Verification	Compliance (Yes/No/NA)
2.1 IDENTITY VERIFICATION GUIDELINES			
1.1(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.*	This text should be clearly displayed in the subscriber software interface.	
1.2(3)	Prior to submitting information for the eKYC account creation of an applicant, the CA shall authenticate the applicant using the applicant's mobile number and the same mobile number shall be used in the subsequent authentication also. Upon successful authentication of the applicant, start a new session for all the associated with the eKYC account creation process and continue the session till its completion. Also, the same mobile number should be a part of the eKYC account of the applicant.	1. Apart from the applicant's mobile number, no other mobile number should be accepted by the software for initial and subsequent authentication. 2. A new session must be initiated for all activities associated with the eKYC account creation process and should continue until the data capture is complete.	
1.2(4)	For eKYC account creation, CA shall provide the interface only to the applicant. Also, CA shall not provide any provision to submit the applicant's details other than the applicant.	Only the applicant should be able to submit the eKYC account creation information.	
1.2(5)	The DSC applicant's access to the website of CA for submission of details for eKYC account creation, video verification and Online Aadhaar authentication shall be only	The CA should prohibit independent link-based access to their eKYC account creation application interface.	

	through a single & dedicated interface provided by CA and link-based access shall not be permitted for these interfaces.		
1.2(6)	In case eKYC account holder requires more than one account (for e.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)	Personal and organizational accounts should be logically visible under a single account.	
1.2(7)	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.	The implementation should have enforced the validity	
1.2(9)	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.	Verify that the applicant has the option to read the agreement and to either accept or reject the application.	
1.2(10)	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.	Verify the availability of the option to access notifications, review the history of eSign transactions, make account modifications, view activation and deactivation information, and manage any queries or disputes through the eKYC account maintained by the CA.	
1.2(11)	Applicant shall have an option to activate, deactivate and close account at any point.	Examine the possibility of activating, deactivating, or closing the account at any given time.	
1.2(12)	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.	Verify the implementation of strong fraud detection and security measures to prevent enrollment frauds. Specifically, the CA should ensure that the page capturing the PIN is protected against phishing attacks, malicious plug-ins, hijacked clicks, and keystrokes.	
1.2(14)	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.	verify the compliance with the format of the eKYC account ID.	

1.2(15)	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.	Inspect the two factor authentication for PIN reset- OTP & email or OTP & face match. Iin the of Banking it should be fresh eKYC.	
1.3(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.	After the CA's approval, two-factor authentication is required for generating the DSC application form	
1.4(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.	The implementation of this control applies to the DSC application form for each type of certificate, including personal signature, organizational signature, encryption, document signer, system certificate, etc	
1.4(2)	For all categories of DSC applicants, it is mandatory to provide either PAN or Aadhaar Number.	CA do not allow the creation of a DSC without providing PAN or Aadhaar information	
1.5(1)	The name of the DSC applicant shall be same as the name in respective eKYC	Name changes should not be permitted by the CA	
1.7(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.	To verify mobile number possession, the CA will send an SMS OTP, which must be captured through the CA-provided interface. The OTP will be random, sent exclusively to the verified mobile number, and not based on predetermined parameters to prevent compromise.	
1.8(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.	The applicant's email address is required for DSC issuance via the eKYC account activated by the CA, but it's optional for eKYC accounts activated solely for eSign purposes.	
1.8(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.	CAs must implement measures to guarantee that email addresses associated with Digital Signature Certificates (DSC) are unique to each DSC applicant. eKYC database should not contain unique email corresponding to different DSC applicant.	

1.8(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.	DSC applicant can have multiple certificate with same name &email id.	
1.8(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.	Send the Email OTP solely to the email address of the DSC applicant, and not to any other address.	
1.8(5)	No disposable email (fast temporary email without registration) shall be accepted by CA.	Verify that the software includes a disposable email check and that the list of disposable emails is updated regularly	
1.9(1)	CA shall electronically verify the PAN number through the eKYC service provided by Income tax and accept only if the verification is successful, the name of the PAN holder and Date of Birth match and also the Aadhaar seeding status is operative. CA shall preserve the proof of verification with their digital signature.	Verify that 1. the CA electronically verifies the PAN number using the eKYC service from the Income Tax department. Acceptance of verification depends on matching the PAN holder's name and date of birth, along with an operative Aadhaar seeding status 2. The CA maintain proof of verification with their digital signature. 3. The exemption from the Aadhaar seeding status is granted solely in accordance with government directives.	
1.10(1)	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.	Verify that the CA conducts: 1. Verification of digital signatures. 2. Automatic population is restricted to digitally signed information only, with no other data permitted	
1.11(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.	Check for photo match during subsequent verifications for changing already registered information or as indicated in the respective section	

1.11(3)	CA shall check any indication of alteration or falsification in video recording	Visual check by CA trusted person.	
1.12(1 & 2)	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. If applicable, the originals of the identity and address proof shall be verified during the video verification	Verify the following: 1. Provision to upload digitally signed documents. 2. Verification of the issuer's digital signature. 3. Cross-verification of uploaded documents with originals shown in the video.	
1.12(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.	For applicable online database verifications on the website, the CA shall retain proof with their signature	
1.12(5)	For the digitally signed documents received from the issuing authority or the same fetched through Digi locker by CA, further verification of supporting documents through video is not required.	The issuer's signature shall be verified for digitally signed documents.	
1.13(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.	Verify the following: 1. The CA client software ensures the private key is generated only on a FIPS 140-2 Level 2/3 validated crypto device. 2. The CA provides Class 2 and Class 3 OIDs in the certificate.	
1.13(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).	Same as 1.13(1)	
1.13(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	1. Verify that the software has the functionality to issue a certificate for the remaining period at least once. 2. Ensure that the CA software does not allow the use of default passwords.	

	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)CA shall not allow the download of DSC to crypto token having default password.		
1.13(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.	Verify that the list of approved cryptographic device manufacturers and suppliers is available on the CA's website	
1.13(5)	For personal signing certificates, subscribers' key generation shall be strictly using the software provided by CA and shall not be generated outside of the crypto device.	1. Verify that for personal signing certificates, subscribers' keys are generated exclusively using the CA-provided software and not outside the crypto device. 2. Ensure the client software has undergone a security audit.	
1.13(7)	Terms and conditions for the use of HSM for class 3 Organisational Person DSCs on FIPS 140-2 level 2/3 certified HSMs shall be as per Annexure-II.	The terms and conditions for using HSM for Class 3 Organizational Person DSCs on FIPS 140-2 Level 2/3 certified HSMs shall be as specified in Annexure-II only	
1.14(1)	To ensure there is no tax evasion in the DSC issuance service a) For Personal Digital Signature Certificate issuance (Class 3), CA shall generate, issue and send the GST tax invoice to the DSC applicant through email. b) For Organizational Person Digital Signature Certificate issuance (Class 2 and Class 3), CA shall generate, issue and send the GST tax invoice to the DSC applicant or applicant's organization through email. c) Except in the case of organisation person certificate through the organization, GeM, tender, person authorized by the organization, etc, CA shall not accept the payment towards DSC issuance in advance, directly or indirectly, causing financial liability in any manner, before the mobile authentication of the DSC applicant.	Verify the software to ensure the provisions mentioned under this section has been implemented. • Confirm that the software automatically generates GST tax invoices for all DSC issuance transactions. • Ensure the software system is configured to send invoices to DSC applicants via email upon issuance. • Template Check: Verify that the software uses a standard TAX invoice template that includes all required GST details (CA name, GSTIN, DSC applicant's details, amount, etc.). • Check software logs to ensure invoices are emailed to the registered email addresses of DSC applicants.	

	CA shall carry out periodic reconciliation of invoices with corresponding DSC issued to subscribers. The copy of the TAX invoice shall be preserved by CA. The applicant's interface software should be integrated with the payment gateway for accepting fees from DSC applicants for the issuance of certificates.	• Verify that the software can send invoices to either the DSC applicant or their organization as required. • Ensure the software is configured to block payment acceptance before mobile authentication of the DSC applicant, except for specific authorized cases (e.g., via GeM, tenders). • Check software logs for evidence of mobile authentication prior to payment acceptance. • Confirm the integration of mobile authentication systems with the DSC issuance software. • Ensure the software includes a feature for periodic automatic reconciliation of issued invoices against corresponding DSCs. • Review generated reconciliation reports for accuracy. • Verify that the software systematically preserves copies of all GST tax invoices in a secure and retrievable manner. • Verify that the software is integrated with a payment gateway for fee acceptance. • Ensure the software maintains detailed logs of all transactions processed through the payment gateway. • Ensure the audit trail includes timestamps and user actions for full traceability. • Verify that the software has appropriate access controls to prevent unauthorized access and modifications. • Check records of user training sessions to ensure staff are properly trained on using the software.	
1.15(1)	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.	Verify the software blocks eKYC service activation until a digitally signed subscriber agreement is confirmed.	

1.16(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	• Ensure the software enforces a 30-day time limit for DSC downloads from the date of verification/approval. • Verify that the software triggers the required eKYC verification processes if the DSC is not downloaded within the 30-day period.	
1.17(1)	CAs shall preserve the digitally signed documents, proof of verification information, logs etc. as per the requirements mentioned in the Information Technology Act.	Verify the software preserves documents , proof of verification information, and logs, digitally signed by a trusted person , according to the requirements of the Information Technology Act.	
1.18(1)	CA shall make sure that the CA Verification Officer's roles and responsibilities are not be delegated or controlled by anyone else.	Ensure the software prevents delegation or control over the roles and responsibilities of CA Verification Officers, making their authority non-bypassable.	
1.18(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.	Validate that the software includes a mechanism to verify the identity of CA Verification Officers	
1.18(3)	CA trusted person/Verification Officer shall approve and certify each account information including name timestamp etc. using their own digital signature	Ensure the software requires each account information approval, including name and timestamp, to be certified by a CA trusted person/Verification Officer using their own digital signature.	
1.19(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.	Confirm that the CA provides a designated software interface enabling users to submit the necessary additional information required for special purpose certificates.	
1.19(2)	Only organisational persons are allowed to apply for special purpose certificate.	User Interface should allow only organizational person	
1.19(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.	Only verified information shall be present in the CA eKYC database.	

1.20(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.	CA escrow facility verification CA verification prior to allow the download of encryption keys	
1.21(1)	The first factor authentication to eKYC account shall be PIN	verify the mandatory first factor authentication facility provided by the CA software	
1.22(1)	The second factor authentication can be SMS-OTP or the other authentication mode specified in the eSign API	The implementation of the second factor authentication.	
1.22(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.	The implementation of the same need to be tested and verified	
1.23(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. Each OTP shall have four digit random identification number	The OTP message should contain PURPOSE. The OTP should be newly generated random number. The OTP message should contain four digit identification number.	
1.23(2)	OTP shall be sent only to the verified mobile number registered in the eKYC account.	The mobile OTP should be sent only to the verified mobile of the subscriber.	
1.24(1)	The role of RA is strictly restricted as a business partner. For business-related accounting purposes, the reference code of RA may be included in the DSC applicant's interface.	CA software should not have provision to access for the submission of details to CA for eKYC account creation for any person other than DSC applicant.	
1.25(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.	CA software shall have provision for this additional physical verification based DSC issuance.	
2.1(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).	The DSC applicant should be able to perform two factor authentication to access the eKYC account and request for DSC after the completion of verification by CA.	

2.1(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.	There should not be any deviation to the format specified Verify as per the subsections of 2.1(2)	
2.2.1(3)	In the case of online Aadhaar Biometric/OTP-based eKYC account enrollment, in addition to the UIDAI requirements a) CA shall ensure that the applicant is already authenticated and started a session as per 1.3(3). b) CA shall start a new session and redirect the user to the dedicated CA interface page for capturing authentication information. (Aadhaar no, Biometric or OTP, consent, etc) . c) For each eKYC request to UIDAI, CA should implement validations at the server side which shall include parent page validation, CA OTP, captcha and session validation prior to submitting the request to UIDAI. d) Only one Aadhaar authentication shall be processed per one session and session time shall be limited to 10 minutes. e) The Aadhaar Number shall not be displayed on the user interface. Only the Name, Last four digits of the Aadhaar and photo shall be displayed to the DSC applicants. f) CA shall look for any external sites linking to them in an unauthorized manner and consuming the purpose by spoofing or scraping the CA website/application. CA shall ensure that they use captcha implementation or similar security to avoid automated attacks and ensure only a human is doing the process on CA enrolment application steps.	Redirect user to the page capturing Aadhaar information Verify as per the subsections of 2.2.1(3)	

	The request for Aadhaar authentication shall only be accepted directly from the CA-controlled application.		
2.2.1(4)	Up on the receipt of Aadhaar eKYC XML from UIDAI, CA decrypts and validates the UIDAI signature, reads and extracts demographic data, and photo.	Verify. Additionally CA should have complete control over the page capturing Aadhaar information	
2.2.1(5)	The verified information received through online Aadhaar e-KYC shall be used for creation eKYC account of user.	For an eKYC account, no changes are allowed to the information received from UIDAI.	
2.2.1(6)	The DSC application form should be generated by populating the information received from UIDAI.	No information change in the DSC application also	
2.2.1(7)	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.	Based on verified information, eSign can be performed only on the DSC application form .	
2.2.1(8)	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.	Additional information like PAN is allowed	
2.2.1(10)	For DSC issuance, email shall be included in the eKYC account after verification by CA.	Email verification is mandatory	
2.2.1(11)	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.	The usage of CA eKYC service only after digitally signing the agreement.	
2.2.1.1(2)	Up on successful authentication, CA receive Aadhaar e-KYC XML and create e-KYC account for the applicant.	eKYC account creation based on Aadhaar e-KYC XML and no modification to the information receiced from UIDAI	
2.2.1.1(3)	The mobile number is mandatory. CA shall capture the mobile number of the user and carryout verification of Mobile Number.	Possession of mobile number with the applicant.	
2.2.1.1(4)	CA does interactive video verification (Annexure VI) and also does a photo match of Aadhaar eKYC photo with the video.	photo match of Aadhaar eKYC photo with the video.	

2.2.1.1(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.	If the video verification Aadhaar Biometric Authentication carried out is more than 2 days old, a fresh video verification/ Aadhaar Biometric Authentication	
2.2.2(1)	It is assumed that subscriber has downloaded digitally signed eKYC XML	Subscriber to download Aadhaar eKYC XML	
2.2.2(2)	Subscriber uploads eKYC XML within CA app/website and provides the "share code/phrase" which is used to encrypt the offline KYC XML.	Submit password to CA	
2.2.2(3)	CA decrypts XML, validates UIDAI signature, reads the Aadhaar eKYC XML, and extracts demographic data, mobile number (when available), and photo.	Validate UID signature and extracts information	
2.2.2(4)	CA shall accept the mobile number within offline KYC only, no changes are allowed.	No Change in Mobile Number	
2.2.2(5)	For issuance of DSC, CA captures email for communications, alerts, and PIN reset options and it must be verified.	email is mandatory	
2.2.2(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.	PAN verification & Name match with Aadhaar eKYC XML	
2.2.2(7)	Subscriber sets up initial PIN and user ID.	Verify the mandatory user input options for PIN and user ID.	
2.2.2(8)	CA does interactive video verification (Annexure VI) and also does a photo match of Aadhaar eKYC photo with the video.	Video & photo match of Aadhaar eKYC photo with the video.	
2.2.2(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.	Verify validation imemented in the software in respect of 2 days.	

2.2.2(10)	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.	Verify the flow	
2.3(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.	The software should not accept residence address for organizational certificates.	
2.3(2)	The minimum requirements for Issuance of DSC to organisation person include: eKYC account of Applicant Applicant ID Proof or Proof of individuals association with organisation Letter of Authorization by Organization to Authorized Signatory for self authorisation and also to other DSC applicants. eKYC account of Authorized Signatory and authorization to DSC applicant Proof of existence of organization	Verify the software implementation of the same	
2.3(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.	Application check implemented for this requirement	
2.3(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.	Verify the mandatory fields	
2.3(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.	Verify the completeness of the sequence	
2.3(9)	CA shall provide Organizational eKYC applicant to set up PIN and user ID upon the authentication by CA.	The PIN and user ID and its usage need to be verified	
2.3(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.	Verify the software implementation for accepting the changes with the authorization of authorised signatory.	

2.3(11)	CA shall accept the mobile number within Organisational KYC only, no changes are allowed.	No provision for changing the mobile number	
2.3(12)	For DSC issuance, the video verification shall have carried out within last 2 days	The application should not accept if the video is more than two days old.	
2.3.1(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.	Verify the option for application to keep the proof of verification and its linking the applicant.	
2.3.1(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	Verify the authorized signatory certificate and the presence of OID in the certificate.	
2.3.1(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.	The provision in the application for the storage of information verified from the website.	
2.4(2)	CA shall verify the source of the request and signature of bank prior to accept KYC information	Verify the implementation of the source checking	
2.4(5)	The DSC to be used for signature by bank shall be registered with CA and shall be mapped with the bank ID/Name	Verify the DSC contents	
2.4(6)	The KYC details shall include Name, address, photo, PAN/Aadhaar Number(last four digit), mobile no, Bank account No, Bank IFSC code (if applicable).	Verify the provision in the application for capturing the KYC details	

2.4(7)	The mobile number and PAN/Aadhaar Number(last four digit) of the applicants are mandatory	Verify the implementation of mandatory fields	
2.4(8)	CA shall allow eKYC applicant to set up PIN and user ID up on the authentication by CA.	PIN and user ID	
2.4(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.	Verify the completeness of the sequence	
2.4(10)	CA shall accept the mobile number within bank KYC only, no changes are allowed.	No provision for change in Mobile Number.	
2.4(11)	For each DSC issuance, CA shall have received KYC of the account holder from the Bank within last 24 hours.	Verify the check implemented	
2.5(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	Check implemented for the mandatory fields	
2.5(4)	The mobile number should have registered in the name of eKYC applicant and the same shall be verified by CA through the services provided by Telecom companies. Or CA should use banking penny drop process to cross verify the name of the DSC applicant with the name registered in the bank account. The proof of the verification shall be preserved	Verify the implementation of telephone verification and banking penny drop process for the conformation of name.	
2.5(6)	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.	Check the implementation of PAN verification service.	
2.5(9)	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.	Verify the digital signature and flow	

2.5(10)	In case of any change in account holder's information after activation of account, CA shall carry out fresh enrollment.	No modification allowed -verify	
2.5(11)	CA shall allow eKYC applicant to set up PIN and user ID up on the authentication by CA.	Provision for setting up PIN and user ID	
2.6(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.	Verify the application interface for capturing the details.	
2.6(3)	For organisational person certificate, Scanned copy of organisational id, organisational email id, mobile number, organisational address and letter of authorization from organisation are required. For the proof of organisational existence, publically verifiable and listed/recognized by local government reference of organisation in database/registry shall be provided. 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.	Verify the application interface for capturing the details.	
2.6(4)	For Personal certificate For identity proof, the scanned copy of Passport/Local Govt issued identity/PAN/OCI passport can be submitted. 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	Verify the application interface for capturing the details.	
2.6(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.	Verify the retention of telephonic verification	

2.6(8)	In case of any change in account holder's information after activation of account, CA shall carry out a fresh enrollment.	No provision for modification after enrollment.	
2.6(9)	CA shall allow eKYC applicants to set up a PIN and user ID upon the authentication by CA. Except in the case of mobile number verification, OTP can be sent to the email of the eKYC user.	mobile verification through email OTP	
2.6(10)	During the validity period of eKYC account, a fresh video verification shall have carried out for each DSC issuance within last 2 days.	Verify the controls implemented to check the validity of the already captured video for DSC issuance.	
3.2(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	Check implemented to ensure the Document Signer certificate is only for organizational person	
4(a)	Applicant's email or mobile numbers are pre-requisites for issuance of Digital Signature Certificate through Aadhaar e-KYC verification channel.	Check the implementation of mandatory fields	
4(e)	The DSC application form should be generated by submitting Aadhaar number of subscriber and populating the information received from UIDAI and the application should be signed by DSC applicant. Additional information like PAN, class of DSC etc should be verified online.	Verify that CA implemented the same using eKYC account creation .	
4(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	Verify the implementation	
4(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.	check the implementation of proof of verification	

4(h)	In the case of organizational person certificates, the DSC application form shall mandatorily be 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.	Verify the implementation.	
Ann II	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.	Check the interface and authorisation	
Ann II(6)	For individual signing certificates, CA should verify the validity of the Key attestation by HSM and also verify no certificates with different DN has been issued earlier.	Verify the key attestation procedure followed by CAs	
Ann III(1)	For GST verification, CA shall be ASP/GSP of GST-GSP where GSP application expose GST System functionalities to ASP/GSP	Verify one sample GST verification for the steps Ann III(1-6)	
Ann III(2)	CA shall use only the organisational GST details verification services provided by GST or their approved GSPs through APIs	Ref Ann III(1-6)	
Ann III(3)	The organisational details include Organisation Name (Legal Name of the Organization), Address & status (active/non-active) at the time of verification.	Ref Ann III(1-6)	
Ann III(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.	Ref Ann III(1-6)	
Ann III(5)	CA shall preserve the digitally signed proof of organisational GST details obtained from GST services.	Ref Ann III(1-6)	
Ann III(6)	The proof of verification shall be digitally signed by the CA.	Ref Ann III(1-6)	

Ann VI(1)	CA shall make available a tamper proof video capture facility in their application.	Perform one video verification and verify the steps Ann VI(1-14)	
Ann VI(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.	Ref Ann VI(1)	
Ann VI(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.	Ref Ann VI(1)	
Ann VI(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.	Ref Ann VI(1)	
Ann VI(5)	If automated video verification is not implemented, at least 2 trusted persons shall independently verify KYC data against video.	Ref Ann VI(1)	
Ann VI(6)	CA shall not make available option for uploading offline video recording and also shall not accept offline recording by any other means.	Ref Ann VI(1)	
Ann VI(7)	CA should allow only one-way video recording session with applicant.	Ref Ann VI(1)	
Ann VI(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.	Ref Ann VI(1)	
Ann VI(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	Ref Ann VI(1)	

	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.		
Ann VI(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	Ref Ann VI(1)	
Ann VI(11)	CA shall carryout cross checking against earlier approved videos of the same applicant to avoid any duplication	Ref Ann VI(1)	
Ann VI(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.	Ref Ann VI(1)	
Ann VI(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.	Ref Ann VI(1)	
Ann VI(14)	From 01.05.2024 onwards, in addition to the existing verification procedures, CA's approval shall include at least 6 second video of the trusted person with specifically reading the random code used in the video verification& application ID. CA shall preserve the digitally signed and timestamped copy of the recordings along with applicants' verification records.	Ref Ann VI(1)	

2.2 eSign API 1.2

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
3.2	eSign service is exposed as stateless service over HTTPS	Verify the implementation	
3.2	it is essential that the requests and responses are digitally signed.	Verify the implementation	

3.2	The usage of HTTPS shall ensure transport layer encryption, while digital signing of XML shall ensure integrity & authenticity of data.	Verify the implementation	
3.3	If eSign user does not provide this explicit consent, application SHOULD NOT process data using this API. ASP front-end application must ensure it takes an "explicit informed signatory's consent" authorizing the ESP to retrieve the resident data, DSC application form generation and submission, key-pair generation, CSR request to CA, Digital Signature on the hash submitted and key pair deletion after Digital Signature creation	Verify the implementation	
DATA FLOW	1.ASP client application asks eSign user to sign the document	Verify the implementation	
DATA FLOW	2.ASP client application creates the document hash (to be signed) on the client side	Verify the implementation	
DATA FLOW	3.ASP client application asks the eSign user to provide consent for certificate generation and signature	Verify the implementation	
DATA FLOW	4.ASP forms the input data for eSign API	Verify the implementation	
DATA FLOW	5.ASP redirect to ESP's URL or uses ESP's SDK application and submit request XML a. ESP validates the calling application and the input. b.ESP verifies the Digital signature of ASP for eSign XML received c.ESP logs the transaction d.ESP redirects eSign user to e- authentication page e.ESP performs authentication and get e-KYC information from e-KYC provider f.ESP show the document hash along with document information to eSign user.	Verify the implementation	

	g.ESP creates a new key pair and CSR for eSign user. h.ESP calls the CA service and gets a Digital Signature Certificate for eSign user. The certificate will be a e-KYC class Digital Signature Certificate, which has e-KYC number, Name of the eSign user, e-KYC response code, Authentication Type, and Time Stamp embedded. i.ESP signs the 'document hash' and provides response XML to the ASP by redirecting to ASP's response URL.		
DATA FLOW	6.ASP receives the document signature and the eSign user's Digital Signature Certificate.	Verify the implementation	
DATA FLOW	7.ASP client application attaches the signature to the document.	Verify the implementation	
DATA FLOW	8.eSign user can accept or reject the signature and DSC	Verify the implementation	
Input/Output of eSign Transactions	1.OTP REQUEST	Verify the implementation	
Input/Output of eSign Transactions	2.OTP RESPONSE	Verify the implementation	
Input/Output of eSign Transactions	3.KYC REQUEST.XML (requests and responses are digitally signed)	Verify the implementation	
Input/Output of eSign Transactions	4.KYC RESPONSE.XML	Verify the implementation	

Input/Output of eSign Transactions	5.ESIGN REQUEST.XML as per 3.3 of eSign API	Verify the implementation	
Input/Output of eSign Transactions	6.FORMC	Verify the implementation	
Input/Output of eSign Transactions	7.CA REQUEST.XML	Verify the implementation	
Input/Output of eSign Transactions	8.CA RESPONSE.XML	Verify the implementation	
Input/Output of eSign Transactions	9.ESIGN RESPONSE.xml as per 3.4of eSign API	Verify the implementation	
Transaction logs	1 Integrity of logs of an eSign Transaction	Verify the implementation	
Transaction logs	2 Archival & Retrival of Logs	Verify the implementation	
Transaction logs	3 Time Source and Accuracy	Verify the implementation	
Transaction logs	4 Signature on a PDF document by ASP	Verify the implementation	
Transaction logs	5 Signature as per the LTV format	Verify the implementation	

2.3 eSign API 3.3

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
	eSign service is exposed as stateless service over HTTPS.	Verify the implementation	
	it is essential that the requests and responses are digitally signed.	Verify the implementation	
	ESP facilitates authentication of eSign user by calling authentication URL of eKYC provider. The e-KYC response will be received by ESP and performs eSign on the eSign request received from ASP within permissible time limit.	Verify the implementation	
	The eSign service API can be used in the scenario where ASP initiates eSign request and ESP authenticates user for eKYC before eSign through eKYC provider.	Verify the implementation	
DATA FLOW	In this scenario: 1. ASP client application asks eSign user to sign the document	Verify the implementation	
DATA FLOW	2. ASP client application creates the document hash (to be signed) on the client side	Verify the implementation	
DATA FLOW	3. ASP client application asks the eSign user id for certificate generation and signature.	Verify the implementation	

DATA FLOW	4. ASP forms the input data for eSign API	Verify the implementation	
DATA FLOW	5. ASP calls ESP's URL and submit request XML a. ESP validates the calling application and the input. b. ESP verifies the Digital signature of ASP for eSign XML received c. ESP logs the transaction d. ESP acknowledges the request back to ASP by providing an ack response with same txn ID. At this time ASP can close the connection to ESP. 6. ASP redirects the user to ESP's authentication page. Alternatively, User can use ESP's mobile app to authenticate. ASP shall suitably display necessary information. a. ESP displays e-authentication page (if web flow) or notifies on ESP mobile app to the eSign user. b. ESP performs authentication using OTP (SMS/TOTP for web flow or OTP bound token for ESP mobile app) along with PIN and get e-KYC information from e-KYC provider. c. ESP shows the document hash along with document information to eSign user. d. ESP creates a new key pair and CSR for eSign user. e. ESP calls the CA service and gets a Digital Signature Certificate for eSign user. f. ESP signs the 'document hash' g. ESP calls ASP's response URL or redirects to response URL (which was part of eSign request) with signed XML response. h. If ASP has provided 'redirectUrl', ESP redirects the user back to ASP's web page (web flow). i. In case response is not received by ASP or user session ends within ASP, ASP can check status of signing request using "checkStatus" API using the same txn ID of the request.	Verify the implementation	

DATA FLOW	7. ASP receives the document signature and the eSign user's Digital Signature Certificate.	Verify the implementation	
DATA FLOW	8. ASP client application attaches the signature to the document.	Verify the implementation	
DATA FLOW	9. ASP shall provide a choice to user to obtain signed document via email, download, short URL sent via SMS, etc.	Verify the implementation	
3.3.1.	eSign XML structure as per 3.3.1.	Verify the implementation	
3.4.	User Authentication Page as per 3.4.	Verify the implementation	
3.5.	Response Data Format - eSign Service as per 3.5.	Verify the implementation	
3.6	. eSign API: Check Signing Status - Request as per3.6	Verify the implementation	
4.1	Functions of eKYC Service : eKYC Service shall operate with the minimum required functions. The functions shall include: 1. Creation of eSign user account 2. Fetch eSign / KYC user information by ESP / CA systems (with user authentication) 3. Perform user Authentication 4. eSign user functionalities	Verify the implementation	
4.2.1.	Aadhaar Offline XML as per4.2.1.	Verify the implementation	
4.2.1.1.	Towards the verification of Aadhaar Offline XML, below minimum steps shall be implemented: a. Validate the Digital Signature of the XML to avoid any tampering.	Verify the implementation	

	b.Validate that it is digitally signed using UIDAI public key certificate, as published by UIDAI. For this purpose, CA may maintain pre-mapped list of valid UIDAI certificates, and update it time-to-time. c.The date of such XML shall be within the prescribed limits by Identity Verification Guidelines (If any). d.Field level verifications as mentioned in above table.		
4.2.2.	Bank eKYC as per4.2.2.	Verify the implementation	
4.2.2.1	Towards the verification of Bank eKYC , below minimum steps shall be implemented: a.Validate the Digital Signature of the XML to avoid any tampering. b.Validate that it is digitally signed using Bank's public key certificate, as provided by respective Bank. For this purpose, CA shall maintain pre-mapped list of valid Bank certificates, and update it time-to-time. c.The date of such XML shall be within the prescribed limits by Identity Verification Guidelines (If any). d.Field level verifications as mentioned in above table.	Verify the implementation	
4.2.2.2.	Bank KYC Request XML Structure: as per 4.2.2.2.	Verify the implementation	
4.2.2.3.	Bank KYC Response XML Structure4.2.2.3.	Verify the implementation	
4.2.3.	Organisational KYC as per4.2.3.	Verify the implementation	
4.2.4.1.	Organisation as per4.2.4.1.	Verify the implementation	

4.2.4.2	.Authorised signatory as per4.2.4.2	Verify the implementation	
4.2.5.	PAN KYCas per	Verify the implementation	
4.2.6	eKYC for foreign Nationals as per	Verify the implementation	
4.3.2	SMS-OTP Functionality rquirements as per 4.3.2.1. Implementation Requirements	Verify the implementation	
4.3.2.2	. Initial registration for this second factor as per	Verify the implementation	
4.3.3	TOTP Implementation Requirements ,Initial registration for this second factor and Authentication Value for this second factor as per 4.3.3. T-OTP Functionality	Verify the implementation	
4.3.4	Mobile Access Tokens Implementation Requirements ,Initial registration for this second factor and Authentication Value for this second factor 4.3.4. Mobile Access Tokens	Verify the implementation	
4.3.5	FIDO Implementation Requirements ,Initial registration for this second factor and Authentication Value for this second factor 4.3.5. FIDO	Verify the implementation	
4.3.6	Public Key Authentication Implementation Requirements ,Initial registration for this second factor and Authentication Value for this second factor 4.3.6. Public Key Authentication	Verify the implementation	

4.4.	4.4. Access to eKYC data The audit logs (both success & Failure) of eKYC user authentications shall be maintained by eKYC Provider with timestamp and user id. The maximum retries with failed authentication by a user (for specific transaction) shall be limited to 5 attempts. eKYC user shall be successfully authenticated as per the multi factor requirements, before accessing KYC information for transactional purposes.	Verify the implementation	
4.4.	The Authentication of the user can happen in Composite or Independent AS PER 4.4.	Verify the implementation	
4.4.1.	eKYC endpoint AS PER 4.4.1.	Verify the implementation	
4.4.2.	eKYC request format as per 4.4.2.	Verify the implementation	
4.4.3.	Second Factor Authentication format as per 4.4.3.	Verify the implementation	
4.4.4.	eKYC response format as per 4.4.4.	Verify the implementation	
4.5.	Subscriber Functionalities as per 4.5.	Verify the implementation	
5	Error Codes as per 5	Verify the implementation	

2.4 Interoperability Guidelines

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
Field Definitions	Validity Subject Subject Public Key Info Unique Identifiers signatureAlgorithm SignatureValue	Generate sample and check the compliance	
Standard Extensions Definition	Standard Extensions Authority Key Identifier Subject Key Identifier Key Usage Certificate Policies Policy Mappings Subject Alternative Name Subject Directory Attributes Basic Constraints Name Constraints Policy Constraints Extended Key Usage CRL Distribution Point Inhibit Any Policy Freshest CRL SignedCertificateTimestampList	Generate sample and check the compliance	
Pvt. Internet Extension	Authority Information Access Subject Information Access	Generate sample and check the compliance	

Annexure I – Issuer and Subject field specification	Naming Conventions Attribute values shall be encoded as specified below:	Verify the compliance in the implementation	
	Specifications for Issuer and Subject DN	Verify the compliance in the implementation	
	CA Certificate – SUBJECT specifications	Verify the compliance in the implementation	
	Sub-CA Certificate – Issuer specifications	Verify the compliance in the implementation	
	Sub-CA Certificate – Subject specifications	Verify the compliance in the implementation	
	End User Certificate (Issued by a Sub-CA) – Issuer specifications	Verify the compliance in the implementation	
	End User Certificate –Subject Specifications	Verify the compliance in the implementation	
Annexure II - Special Purpose Certificates	1. SSL Certificate	Check the implementation and output to see the compliance	
	System Certificates	Check the implementation and output to see the compliance	
	3. Time stamping authority certificate	Check the implementation and output to see the compliance	
	4. Code Signing	Check the implementation and output to see the compliance	
	5. Encryption Certificate	Check the implementation and output to see the compliance	

	6. OCSP Responder Certificate	Check the implementation and output to see the compliance	
	7. Organisational Document Signer Certificate	Check the implementation and output to see the compliance	
Annexure III - Reference Certificate Profiles	CA Certificate Profile	Check the implementation and output to see the compliance	
	Sub-CA Certificate Profile	Check the implementation and output to see the compliance	
	End User Certificate Profile (issued for personal use)	Check the implementation and output to see the compliance	
	End User Certificate Profile (issued for organization use)	Check the implementation and output to see the compliance	
	SSL Certificate Profile	Check the implementation and output to see the compliance	
	System Certificate Profile	Check the implementation and output to see the compliance	
	Time Stamping Authority Certificate Profile	Check the implementation and output to see the compliance	
	Code Signing Certificate Profile	Check the implementation and output to see the compliance	
	OCSP Responder Certificate Profile	Check the implementation and output to see the compliance	
	Encryption Certificate profile (issued for personal use)	Check the implementation and output to see the compliance	

	Encryption Certificate profile (issued for organisation use)	Check the implementation and output to see the compliance	
	Organisational Document Signer Certificate Profile	Check the implementation and output to see the compliance	
	CRL Profile	Check the implementation and output to see the compliance	

2.5 CPS

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
2.1.1. Repository Obligations	CA maintains a repository and is available at	Test the URL	
3.1.3. Anonymity of Subscribers	CA does not issue subscriber certificates with anonymous identities.	Verify the checks implemented	
3.1.5. Uniqueness of Names	Name uniqueness for interoperability or trustworthiness is enforced in association with a serial number or unique identifier.	Verify the checks implemented	
3.2.1. Method to Prove Possession of Private Key	In all cases where the DSC applicant named in a certificate generates its keys, the DSC applicant is required to prove possession of the private key, which corresponds to the public key in the certificate request. This will be performed by the DSC applicant using its private key to sign a value and provide that value to the issuing CA. The CA then validates the signature using the DSC applicant public key.	Verify how CA implemented the requirements	
4.3. Certificate Issuance	After a certificate applicant submits a certificate application, the CA verifies or refutes the information in the certificate application. Upon successful verification based on all required authentication procedures for various classes of certificates, forward the certificate application for approval. The applicant's request for certificate issuance is reviewed by a trusted person which may result in approval or denial of the certificate. The responses received from publicly available databases, used to confirm Subscriber information, are protected from unauthorized modification	Mainlining the integrity of the eKYC response	
4.3.1. CA Actions during Certificate Issuance	CA verifies the source of a certificate request before issuance. If the crypto medium is used for the key generation and storage, the details such as make, model, serial no, etc are also recorded. Certificates are checked to ensure that all	Examine the implementation to see the information captured.	

	fields and extensions are properly populated. After generation, verification, and acceptance, CA publishes the certificate in the repository.		
4.3.2. Notification to Subscriber of Certificate Issuance	CA will notify the subject (End Entity Subscriber) of certificate issuance through email/SMS and internet link.	Verify the implementation.	
4.9. Certificate Revocation and Suspension	CA authenticates the request for revocation before revocation. Subscribers are required to submit revocation requests as specified under IT CA Rules. Electronic requests to revoke a certificate have to be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.	Verify the implementation of this option.	
4.9.7. CRL Issuance Frequency	CA issues CRLs periodically, even if there are no changes to be made, to ensure the timeliness of the information. Certificate status information may be issued more frequently than the issuance frequency described below. CA ensures that superseded certificate status information is removed from the PKI Repository upon posting the latest certificate status information. CA publishes CRLs no later than the next scheduled update. CA issue CRLs at least once every 24 hours with a minimum validity of 7 days. In addition, CA issues CRLs and posts the CRL immediately if a certificate is revoked for the reason of a key compromise.	Check the implementation as per 4.9.7	
5.2.1 Trusted Roles	A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. The requirements of this policy are drawn in terms of four roles listed below:	Verify the permission given to the role as per 5.2.1	

	1. CA Administrator – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys. 2. CA Officer – authorized to request or approve certificates or certificate revocations. 3. Audit Administrator – authorized to view and maintain audit logs. 4. System Administrator – authorized to perform system backup and recovery.		
5.2.1.1 CA Administrator	The administrator shall be responsible for: 1. Installation, configuration, and maintenance of the CA; 2. Establishing and maintaining CA system accounts; 3. Configuring certificate profiles or templates and audit parameters, and; 4. Generating and backing up CA keys. Administrators shall not issue certificates to subscribers.	Verify the permission given to the role	
5.2.1.2 CA Officer	The CA officer shall be responsible for issuing certificates, that is: 1. Registering new subscribers and requesting the issuance of certificates; 2. Verifying the identity of subscribers and accuracy of information included in certificates; 3. Approving and executing the issuance of certificates, and; 4. Requesting, approving and executing the revocation of certificates.	Verify the permission given to the role	
5.2.1.3 Audit Administrator	The Audit Administrator shall be responsible for: 1. Reviewing, maintaining, and archiving audit logs; 2. Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;	Verify the permission given to the role	
5.2.1.4 System Administrator	The System Administrator shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.	Verify the permission given to the role	
5.2.2. Number of Persons Required per Task	Separate individuals are identified for each trusted role to ensure the integrity of the CA operations. Two or more persons are required to perform the following tasks for CAs that issue Class 1, Class 2, or Class 3 certificates: 1. CA key generation; 2. CA signing key activation; and	Verify the implementations per 5.4.2	

	3. CA private key backup. In addition, sensitive CA operations like operations of the cryptographic units and certificate manager require the m-out-of-n control to handle the operations of these sensitive functions. Also, split control is implemented to ensure segregation between physical and logical access to systems Personnel having secret shares do not have physical access and vice-versa. All roles are assigned to multiple persons to support the continuity of operations.		
5.4.1. Types of Events Recorded	All security auditing capabilities of the CA operating system and the CA applications required by this CPS are enabled. Each audit record includes the following (either recorded automatically or manually for each auditable event): 1. The type of event, 2. The date and time the event occurred, 3. Success or failure where appropriate, and 4. The identity of the entity and/or operator that caused the event	as per 5.4.1.	
5.4.4. Protection of Audit Logs	System configuration and procedures are implemented together to ensure that: 1. Only authorized people have read access to the logs; 2. Only authorized people may archive audit logs; and, 3. Audit logs are not modified. After back-up and archiving, the audit logs are allowed by the system to be over-written.	Verify the implementations per 5.4.4	
5.5.1. Types of Records Archived	Types of Records Archived	Check the records are archived by CA as Per 5.5.1	
5.5.2. Retention Period for Archive	Records associated with certificates are archived for 7 years from the date of expiry of the certificate.	Verify the archival and time stamping	
5.5.5. Requirements for Time-Stamping of Records	Archived records are time-stamped such that the order of events can be determined. Certificates, CRLs, other revocation databases, and usage entries contain time and date information provided by System time, which is synchronized with IST (NPLI).	The proof of synchronization with IST kept by the CA.	

6.1.1. Key Pair Generation	Key Pair Generation	AS PER 6.1.1.	
6.1.2. Private Key Delivery to Subscriber	The subscriber private key is generated by the end subscriber and hence there is no delivery to the end Subscribers. In the case of hardware-based tokens or smart cards, pre-formatted tokens are sent to the Subscribers and the associated PIN is sent by an out-of-band process. The end user then uses the token and the client software provided to him to generate and store the private key and also initiates an online session with the CA server for certificate generation.	Check the mechanism implemented by the CA to ensure that the private key is generated only by the software provided the CAs and securely sending to CA for certification.	
6.1.5. Key Sizes	Key Sizes	Verify the configuration for the support key sizes as per 6.1.5.	
6.2.3. Private Key Escrow	CA creates a backup of its signature keys. These are stored in encrypted form and under the sole custody of CA.	Check the backed-up keys are stored in encrypted form.	
6.2.4.1. Backup of CA Private Signature Key	CA private signature keys are backed up under the same multi-person control as the original signature key. The number of backup copies is limited to three and securely stored under the same multi-person control as the operational key.	Verify the implementation as per 6.2.4.1	
6.2.7. Private Key Storage on Cryptographic Module	CA stores Private Keys in the hardware cryptographic module and keys are not accessible without an authentication mechanism that complies with the FIPS 140-2 rating of the cryptographic module.	Verify the implementation as per 6.2.7	
6.2.8. Method of Activating Private Key	The user must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, Personal Identification Numbers (PINs), or biometrics. Entry of activation data is protected from disclosure (i.e., the data should not be displayed while it is entered).	Verify the implementation as per 6.2.8	

6.2.9. Methods of Deactivating Private Key	The cryptographic module that has been activated is never left unattended or otherwise available for unauthorized access. After use, cryptographic modules are deactivated. After deactivation, the use of the cryptographic modules-based CA key pair requires the presence of the trusted roles with the activation data to reactivate said CA key pair.	Check the configuration as per 6.2.9 for CA	
6.4.1. Activation Data Generation and Installation	The activation data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection. When they are not used, activation data are always stored in a safe for which access is controlled by holders in limited roles.	Verify the CA public key activation involves crypto smart card or not . Check the configuration as per 6.4.1	
6.8. Time Stamping	All CA components are regularly synchronized with a time service such as Indian Standard Time Service. Time derived from the time service is used for establishing the time of: 1. Initial validity time of a Subscriber's Certificate 2. Revocation of a Subscriber's Certificate 3. Posting of CRL updates 4. OCSP	Test and confirm at UAT	
7.3.1. OCSP Request Format	Requests sent to Issuer CA OCSP Responders are not required to be signed. The following table lists the fields that are expected by the OCSP Responder.	Verify as per 7.3.1	
7.3.2. OCSP Response Format	See RFC2560 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.	Verify as per 7.3.2	
9.1.1. Certificate Issuance and Renewal Fees	9.1.1. Certificate Issuance and Renewal Fees	Working link	
9.12.2. Notification Mechanism and Period	Errors and anticipated changes to this CPS resulting from reviews are published online at CA URL This CPS and any subsequent changes are made publicly available within seven days of approval.	Check CA URL is functional Check the CPS Upload date	

2.6 Security Requirements for Crypto Devices

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
2.17 Admin Password feature for USB-based crypto device	b) From 01.04.2023 onwards, CAs shall allow only the download of DSC on the crypto tokens holding the new unique serial number and having no user PIN reset option by any means.	verify	

2.7 X.509 Certificate Policy for India PKI

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
1.3.1.4 Sub-CA	1.3.1.4 Sub-CA The sub-CA model will be based on the following principles: 1. The CAs MUST NOT have more than ONE level of sub-CA 2. The sub-CA MUST use a sub-CA certificate issued by the CA for issuing end entity certificates 3. The sub-CA must necessarily use the CAs infrastructure for issuing certificate 4. The sub-CAs operations shall be subject to same audit procedures as the CA 5. The certificate policies of the sub-CA must be same as or sub-set of the CA's certificate policies	Check whether CA software is allowed to issue more than one level of certificate.	
4.9.8 Maximum Latency for CRLs	CRLs shall be published immediately after generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the	Check CRL next update time	

	previously issued CRL. CAs must issue CRLs at least once every 24 hours, and the nextUpdate time in the CRL may be no later than 7 days after issuance time (i.e., the thisUpdate time).		
4.12.1 Key Escrow and Recovery Policy and Practices	Under no circumstances shall a CA or end entity signature key be escrowed by a third-party.	Check issuance process to ensure that only CSR file is accepted by the CA application for certification.	

2.8 Online Certificate Status Protocol (OCSP)

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
Additional OCSP Service Guidelines	1.The CA SHALL support an OCSP capability using the GET or the POST method for DSC issued under PKI India Hierarchy .	Verify the implementation to make sure GET or POST	
Additional OCSP Service Guidelines	2.The CA SHALL operate OCSP capability to provide a response time of ten seconds or less under normal operating conditions.	Test the response time	
Additional OCSP Service Guidelines	3.OCSP responses MUST be signed by an OCSP Responder whose Certificate is signed by the CA or its subCA that issued the Certificate whose revocation status is being checked.	Inspect the issuer of OCSP certificates to validate the same	
Additional OCSP Service Guidelines	4.In the case of certificates issued under special purpose trust chain for SSL and Code Signing, If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder MUST NOT respond with a "good" status. The CA SHOULD monitor the responder for such requests as part of its security response procedures	Validate the process flow in the case of SSL and code signing certificates	
Additional OCSP Service Guidelines	5. As part of Interoperability initiative, certificates issued by CAs should have id-ad-ocspaccesslocation pointing to the CA's OCSP responder.	Verify all types of certificates issued by CA to check the id-ad-ocspaccesslocation in the certificates	
Additional OCSP Service Guidelines	6. The end to end process must be automated for providing OCSP response to a Relying Party. There must not be any manual intervention unless an error condition arises.	Inspect the process flow	

Additional OCSP Service Guidelines	7. The OCSP must accept both signed and unsigned OCSP requests	Test & verify	
Additional OCSP Service Guidelines	8. The OCSP precomputed or cached responses must have 8 hours validity for CA & Sub CA and one hour validity for end-entity certificates. CA must update OCSP precomputed or cached responses in every 30 minutes	Generate a response and check the caching time applicable for a CA	
Additional OCSP Service Guidelines	9. The OCSP Responder should be able to support nonce extension in request and responses	Generate a response and check nonce	

2.9 Time Stamping Services Guidelines

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
1. Introduction	The Time stamping service provided by CA should be logically & physically separate from the CA systems. However CA can use the same physical infrastructure and resources. The Audit of the Time Stamping service shall be included in the audit of CA facilities.	Inspect the logical& physical isolation	
2 OID	This identifier (i.e., {2.16.356.100.3.0} shall be asserted in every time stamp token.	Check the OID in the time stamp token	
3 Time Stamp Certificate	The Time Stamping certificates shall be issued by an Intermediate CA. An intermediate CA with sub-CA must necessarily issue time stamping certificates only through its intermediate CA.	Check the issuer certificate	

4.1 Time Stamp Token	Time stamp tokens shall be in compliance with RFC 3161. Each time stamp token shall have a unique identifier. The time included in the time-stamp token shall be synchronized with Standard Time Source within the accuracy defined in this policy and, if present, within the accuracy defined in the time-stamp token itself. The accuracy is defined to be ± 1 second. In compliance with RFC 3161, the time-stamp token shall include a representation (e.g., hash value) of the datum being time-stamped as provided by the time stamp requestor/subscriber. The time-stamp token shall be signed using a key generated exclusively for this purpose. The relying parties shall be able to ascertain this by the presence of a critical extended key usage extension of id-kp-timestamping {1 3 6 1 5 5 7 3 8}.	Generate a token & verify the results Check the key is used for any other purpose	
4.2 Time Stamping Services Clock	The time values the Time Stamping services uses in the time-stamp token shall be traceable to a Standard Time Source in India. The Time Stamping services clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration. Examples of threats include tampering by unauthorized personnel, radio or electrical shocks. The CA shall provide a capability to detect the Time Stamping services clock being out accuracy specified in this guidelines. When the Time Stamping services clock is detected as being out of the accuracy specified in these guidelines, the event shall be audited and time-stamp tokens shall not be issued. Furthermore, this non-issuance shall be audited	Test whether applications are configured to accept time other than from the source NPLI. Test whether the time stamping service application detect the accuracy and act	
5.1.1 Types of Events Recorded	All security auditing capabilities of the operating system and the applications required shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event): 1. The type of event, 2. The date and time the event occurred, 3. Success or failure where appropriate, and 4. The identity of the entity and/or operator that caused the event	Chek the transactions and corresponding audit records as per 5.1.1	

6.2.1 Time Request Format	Time stamp requests sent to the CAs are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC 3161 for detailed syntax. The following table lists the fields that are expected by the Time Stamping Services	Verify the request	
6.2.2 Time Stamp Response Format	See RFC 3161 for detailed syntax. The following table lists which fields are populated by the Time Stamping Services.	Validate the response format as per 6.2.2	

2.10 Web Site of the CA

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)
3. Compliance Requirements for the CA Website	1. CA website shall display current past versions of CPS	Verify the availability	
3. Compliance Requirements for the CA Website	2. The repository of CA shall be made available to the public	Verify the availability	
3. Compliance Requirements for the CA Website	3. CA website shall provide a direct interface to applicants. CA web site shall make available the direct payment options to the DSC applicants	Verify the availability	

3. Compliance Requirements for the CA Website	4. CA website shall publish CRL and CA certificate details	Verify the availability	
3. Compliance Requirements for the CA Website	5. A help desk for subscribers and application owners shall be provided and the details should be available on the website of CA	Verify the availability	
3. Compliance Requirements for the CA Website	6. Contact details & email shall be published on the CA website	Verify the availability	
3. Compliance Requirements for the CA Website	7. The website shall provide a Grievance & Redressal interface	Verify the availability	
3. Compliance Requirements for the CA Website	8. The certificate fees shall be made available on the website	Verify the availability	
3. Compliance Requirements for the CA Website	9. The list of empanelled token providers shall be published by CA on their website.	Verify the availability of the list with below third level.	
3. Compliance Requirements for the CA Website	10. CA shall provide a certificate search option for a subscriber based on authentication	Verify the search option for all the certificates issued by the CA to users	
3. Compliance Requirements for the CA Website	11. The website shall provide eKYC account-related information access as mentioned in the IVG	Check the interface to the subscriber	
3. Compliance Requirements for the CA Website	12. Provision for submitting the certificate revocation request by a subscriber shall be provided	Validate the interface and authentication	
3. Compliance Requirements for the CA Website	13. The website should display the list of directors and the authorised representative details	Check this information is available below third level(two click)	

3. Compliance Requirements for the CA Website	14. Ensure that no confidential information is available publically through the CA website	Inspect the website to verify the same	
3. Compliance Requirements for the CA Website	15. Ensure high availability of the CA website at all levels	Validate the high availability	
3. Compliance Requirements for the CA Website	17. Role-wise access control mechanism implemented for the access to the website for updating and administration	Validate the role wise access control to the website	
3. Compliance Requirements for the CA Website	18. CA shall record the non-availability/hacking/other failure-related incidents and the same shall be made available to auditors.	Verify the mechanism implemented for capturing non-availability and failure	
THE INFORMATION TECHNOLOGY (CERTIFYING AUTHORITY) REGULATIONS, 2001	(i) Publication of Public Key Certificate. The Certifying Authority shall, on acceptance of a Public Key Certificate by a subscriber, publish it on its web site for access by the subscribers	Verify the mechanism provided by the CA software for acceptance of certificate.	
Schedule II - NOMINATED WEBSIT	A website designated by the Certifying Authority for display of information such as fee schedule, Certification Practice Statement, Certificate Policy etc.	Inspect the web site to confirm the website is dedicated only for the Licensed CA.	

2.11 CA Services

Control No.	Control	Functional Test/Verification	Compliance (Yes/No/NA)

Web site & Directory	CA web shall be available 24X 7 The disaster Recovery site shall be operational if DC is not operational with out any delay	Verify the availability of the CA website from either DC or DR at all times	
Web site & Directory	Subscriber should be able to submit the revocation at any point of time through CA web interface	Verify	
Web site & Directory	The sub-CA certificate contained in the Authority Information filed of subscriber's certificate shall be accessible irrespective the site is operated from DC or DR	Verify	
CRL	The CRL link contained in the CRL distribution filed of subscriber's certificate shall be accessible irrespective the site is operated from DC or DR	Verify : :There should not be any change in URL of the sub-CA certificate and CRL irrespective of the access from DC or DR	
OCSP	The OCSP source contained in the CRL distribution filed of subscriber's certificate shall be accessible irrespective the site is operated from DC or DR	Verify : the changes should be transparent for the external access.	
OCSP	The OCSP service should be available 24X7 either from DC or DR.	Verify the high availability	
CA software component for key generation	The CA software component provided for key generation should have undergone security testing as per annexure VI of CC-LIC.	verify	

****

1. ANNEXURE - CHECK LIST PAN AUTHENTICATION (PERSONAL)

SL	CHECK POINTS	CCA REMARKS
1.	**GENERAL**	
	Select **Indian** /Foreign	
	Select **personal** /organisational (Authorized Signatory / Employee)	
	Select **class/validity**	
	Select **signature**/encryption	
	Select services(token/ support service)	
	KYC Type (**PAN** / Aadhaar -Offline / online)	
	Display Price	
2	**KYC Enrolment - PAN AUTHENTICATION(PERSONAL)**	
	Mobile OTP authentication – Session start	
	If KYC enrolment page is not called from CA site it should not allow. Link or call to this page not allowed	
	Optionally, display the previously selected general information in an editable form, or provide an option to select general parameters directly here	
	PAN API (PAN, name, and DoB) - verify Aadhaar linking status & apply state exception order. - No option for editing/changing Name - Option for re-authenticate	
	Address	
	Mobile No(Non editable) - Verification[NSDL][OTP]	
	Email – Verification	
	Video verification - option for review- re-verification	
	User ID & PIN	
	Payment & Invoice	
	Upload documents & photo	
	Business Partner(BP) Ref No (optional)	
	Session end	

	DEMONSTRATE	
	1. Mobile no cannot be changed	
	2. Name cannot be changed after pan authentication	
	3. Mobile Number & Name is not editable	
	4. If exit during KYC entry, the already entered information should be available after re-authentication using mobile & OTP	
	5. The option for review- re-verification in video by the applicant	
	6. Disposable email check in email verification	
	7. Option for entering user ID & PIN	
	8. Payment: No independent link on the URL other than from within the CA website	
	9. Upload documents 10. Provision to verify the electronic signature on the electronically signed documents.	
	11. BP is optional	
	12. During the session, input options can be interchanged freely between the start and end	
	13. The invoice includes only charges for DSC/token/support services.	
3.	**CA VERIFICATION**	
	Verify the completeness and accuracy of the information in accordance with IVG.	
	Video verification- All photo IDs and video in a single screen -document verification	
	Mobile Verification using telecom provider service	
	Two level verification	
	Video of the final approver Digital signature of the final Approver.	
	In case of rejection, send a notification to the subscriber to complete it.	
	DEMONSTRATE	
	1. CA verification by CA verification Officer(trusted member) 2. Approval procedure for identifying and checking each CA officer. 3. DSC & Video of the approver	
4	**APPLICANT APPROVAL**	

	Login with USERID, PIN & OTP – session start	
	Display the user agreement & sign	
	CAs approval of KYC account.	
	Applicant generate DSC application form with response code, display & sign	
	CA activate eKYC account -Session end	
	CA enable DSC for download	
	Upon activation of an eKYC account, previously submitted information should only be accessible through the eKYC account.	
	DEMONSTRATE	
	1. Login with two factor authentication by DSC applicant	
	2. eSign on the agreement & option for user to accept or reject	
	3. User see the DSC application form & sign The DSC application form shall mandatorily contain requested DSC details(Class, signature/encryption, validity, Indian etc) , Name , address, Photo, PAN/Aadhaar, response code, email etc as in Form C)	
	4. After eKYC account activation, a. upon authenticating (mobile authentication) with a mobile number and OTP, a fresh entry page should be displayed. b. upon authenticating (eKYC account authentication) with a mobile number, PIN and OTP, the user dash board should be displayed.	
	5. PIN reset.	
	6. During the session, the input options & CA actions are NOT interchangeable between the start and end	
	7. The dash board of the eKYC user	

2. ANNEXURE - CHECK LIST OFFLINE AADHAAR AUTHENTICATION (PERSONAL)

SL	CHECK POINTS	CCA REMARKS
1.	**GENERAL**	
	Select **Indian** /Foreign	
	Select **personal** /organisational (Authorized Signatory / Employee)	
	Select class/validity	
	Select **signature**/encryption	
	Select services(token/ support service)	
	KYC Type (PAN / **Aadhaar -Offline** / online)	
	Display Price	
2	**KYC Enrolment OFFLINE AADHAAR (PERSONAL)**	
	Mobile OTP authentication – Session start	
	If KYC enrolment page is not called from CA site it should not allow. Link or call to this page not allowed	
	Optionally, display the previously selected **GENERAL** information in an editable form, or provide an option to select general parameters directly here	
	Upload Offline Aadhaar XML & PIN	
	Verify that the mobile number used in offline KYC matches the mobile number used for KYC enrolment authentication.	
	PAN API (PAN , name, and DoB) - verify Aadhaar linking status & apply state exception order. - No option for editing/changing Name - Option for re-authenticate	
	Display option for name as in PAN/Aadhaar & change name accordingly (editing is not allowed)	
	Address – As received from UID XML(non editable)	
	Photo - As received from UID XML(non editable)	
	Mobile No- As received from UID XML & (non editable)	
	Email –verification	
	Video verification - option for review- re-verification	
	User ID & PIN	
	Payment & Invoice	
	Upload documents	
	Business Partner(BP) Ref No (optional)	

	Session end	
	DEMONSTRATE	
	1. Aadhaar XML signature verification	
	2. Mobile no , Photo & Address cannot be changed	
	3. Name cannot be changed after pan/Aadhaar authentication	
	4. Mobile Number, Name, photo & Address is not editable	
	5. The authentication mobile matches with the mobile number in the Aadhaar XML	
	6. If exit during KYC entry, the already entered information should be available after re-authentication using mobile & OTP	
	7. The option for review- re-verification in video by the applicant	
	8. Disposable email check in email verification	
	9. Option for entering user ID & PIN	
	10. Payment: No independent link on the URL other than from within the CA website	
	11. Upload documents , if any	
	12. Provision to verify the electronic signature on the electronically signed documents.	
	13. BP is optional	
	14. During the session, input options can be interchanged freely between the start and end.	
	15. The invoice includes only charges for DSC/token/support services.	
3.	**CA VERIFICATION**	
	Verify the completeness and accuracy of the information in accordance with IVG.	
	Video verification- All photo IDs and video in a single screen -document verification	
	Two level verification	
	Video of the final approver Digital signature of the final Approver.	
	In case of rejection, send a notification to the subscriber to complete it.	
	DEMONSTRATE	
	1. CA verification by CA verification Officer(trusted member) 2. Approval procedure for identifying and checking each CA officer. 3. DSC & Video of the approver	
4	**APPLICANT APPROVAL**	
	Login with USERID PIN & OTP – session start	
	Display the user agreement & sign	

	CAs approval of KYC account	
	Applicant generate DSC application form with response code, display & sign	
	CA activate eKYC account -Session end	
	CA enable DSC for download	
	Upon activation of an eKYC account, previously submitted information should only be accessible through the eKYC account.	
	DEMONSTRATE	
	1. Login with two factor authentication by DSC applicant	
	2. eSign on the agreement & option for user to accept or reject	
	3. User see the DSC application form & sign The DSC application form shall mandatorily contain requested DSC details(Class, signature/encryption, validity, Indian etc) Name , address, Photo, PAN/Aadhaar, response code, email etc as in Form C)	
	4. After eKYC account activation, a. upon authenticating (mobile authentication) with a mobile number and OTP, a fresh entry page should be displayed. b. upon authenticating (eKYC account authentication) with a mobile number, PIN and OTP, the user dash board should be displayed	
	5. PIN reset.	
	6. During the session, the input options & CA actions are **NOT** interchangeable between the start and end	
	7. The dash board of the eKYC user	

3. ANNEXURE - CHECK LIST ONLINE AADHAAR(OTP) AUTHENTICATION (PERSONAL)

SL	CHECK POINTS	CCA REMARKS
1.	**GENERAL**	
	Select **Indian** /Foreign	
	Select **personal** /organisational (Authorized Signatory / Employee)	
	Select class/validity	
	Select **signature**/encryption	
	Select services(token/ support service)	
	KYC Type (PAN / **Aadhaar -Offline** / online)	
	Display Price	
2	**KYC Enrolment ONLINE AADHAAR(OTP) (PERSONAL)**	
	Mobile OTP authentication – Session start	
	If KYC enrolment page is not called from CA site it should not allow. Link or call to this page not allowed	
	Optionally, display the previously selected **GENERAL** information in an editable form, or provide an option to select general parameters directly here	
	Aadhaar: Redirect [start session A] user to a CA page for capturing Aadhaar Number, OTP , consent, etc - UID - **Back to KYC enrolment page** with response**[end session A]** If Aadhaar eKYC page is not called from KYC enrolment page it should not allow. Link or independent call to this page shall not allowed Display only last four digit of Aadhaar in the KYC page	
	PAN API (PAN , name, and DoB) (optional) - verify Aadhaar linking status & apply state exception order. - No option for editing/changing Name - Option for re-authenticate	
	Display option for name as in PAN/Aadhaar & change name accordingly (editing is not allowed)	
	Address – As received from UID XML(non editable)	
	Photo - As received from UID XML(non editable)	
	Mobile No- As authenticated & (non editable)	
	Email –verification	
	Video verification - option for review- re-verification	
	User ID & PIN	
	Payment & Invoice	

	Upload documents , if any	
	Business Partner(BP) Ref No (optional)	
	Session end	
	DEMONSTRATE	
	1. Photo & Address cannot be changed	
	2. Display last four digit of Aadhaar in KYC entry page	
	3. Name cannot be changed after pan/Aadhaar authentication	
	4. Mobile Number, Name, photo & Address is not editable	
	5. If exit during KYC entry, the already entered information should be available after re-authentication using mobile & OTP	
	6. The option for review- re-verification in video by the applicant	
	7. Disposable email check in email verification	
	8. Option for entering user ID & PIN	
	9. Payment: No independent link on the URL other than from within the CA website	
	10. Upload documents , if any	
	11. BP is optional	
	12. During the session, input options can be interchanged freely between the start and end.	
	13. The invoice includes only charges for DSC/token/support services.	
3.	**CA VERIFICATION**	
	Verify the completeness and accuracy of the information in accordance with IVG.	
	Video verification- All photo IDs and video in a single screen -document verification	
	Two level verification	
	Video of the final approver Digital signature of the final Approver.	
	In case of rejection, send a notification to the subscriber to complete it.	
	DEMONSTRATE	
	1. CA verification by CA verification Officer(trusted member) 2. Approval procedure for identifying and checking each CA officer. 3. DSC & Video of the approver	
4	**APPLICANT APPROVAL**	
	Login with USERID, PIN & OTP – session start	
	Display the user agreement & sign	

	CAs approval of KYC account	
	Applicant generate DSC application form with response code, display & sign	
	CA activate eKYC account -Session end	
	CA enable DSC for download	
	Upon activation of an eKYC account, previously submitted information should only be accessible through the eKYC account.	
	DEMONSTRATE	
	1. Login with two factor authentication by DSC applicant	
	2. eSign on the agreement & option for user to accept or reject	
	3. User see the DSC application form & sign The DSC application form shall mandatorily contain requested DSC details(Class, signature/encryption, validity, Indian etc) Name , address, Photo, PAN/Aadhaar, response code, email etc as in Form C)	
	4. After eKYC account activation, a. upon authenticating (mobile authentication) with a mobile number and OTP, a fresh entry page should be displayed. b. upon authenticating (eKYC account authentication) with a mobile number, PIN and OTP, the user dash board should be displayed	
	5. PIN reset.	
	6. During the session, the input options & CA actions are **NOT** interchangeable between the start and end	
	7. The dash board of the eKYC user	

4. ANNEXURE - CHECK LIST ON-LINE AADHAAR (BIOMETRIC) AUTHENTICATION (PERSONAL)

SL	CHECK POINTS	CCA REMARKS
1.	**GENERAL**	
	Select **Indian** /Foreign	
	Select **personal** /organisational (Authorized Signatory / Employee)	
	Select **class/validity**	
	Select **signature**/encryption	
	Select services(token/ support service)	
	KYC Type (**PAN / Aadhaar -Online** / online)	
	Display Price	
2	**KYC Enrolment ONLINE-AADHAAR (PERSONAL)**	
	Mobile OTP authentication – Session start	
	If KYC enrolment page is not called from CA site it should not allow. Link or call to this page not allowed	
	Optionally, display the previously selected **GENERAL** information in an editable form, or provide an option to select general parameters directly here	
	Aadhaar : [start session A] Redirect user to a CA page for capturing Aadhaar Number, Biometric , consent, etc - UID - **Back KYC enrolment page** with response **[end session A]** If Aadhaar eKYC page is not called from KYC enrolment page it should not allow. Link or independent call to this page shall not allowed Display only last four digit of Aadhaar in the KYC page	
	PAN API (PAN , name, and DoB) (optional) - Verify Aadhaar linking status & apply state exception order. - No option for editing/changing Name - Option for re-authenticate	
	Display option for name as in PAN/Aadhaar & change name accordingly (editing is not allowed)	
	Address – As received from UID XML(non editable)	
	Photo - As received from UID XML(non editable)	
	Mobile No- As used in authentication(non editable)	
	Email –verification	
	User ID & PIN	
	Payment & Invoice	
	Business Partner(BP) Ref No (optional)	

	Session end	
	DEMONSTRATE	
	1. Mobile no , Photo & Address cannot be changed	
	2. Name cannot be changed after pan/Aadhaar authentication	
	3. Mobile Number, Name, photo & Address is not editable	
	4. Display last four digit of Aadhaar in KYC entry page	
	5. If exit during KYC entry, the already entered information should be available after re-authentication using mobile & OTP	
	6. Disposable email check in email verification	
	7. Option for entering user ID & PIN	
	8. Payment: No independent link on the URL other than from within the CA website	
	9. Upload documents , if any	
	10. BP is optional	
	11. During the session, input options can be interchanged freely between the start and end.	
	12. The invoice includes only charges for DSC/token/support services.	
3.	**CA VERIFICATION**	
	Verify the completeness and accuracy of the information in accordance with IVG.	
	Video verification- document verification (if applicable)	
	Two level verification	
	Video of the final approver Digital signature of the final Approver.	
	In case of rejection, send a notification to the subscriber to complete it.	
	DEMONSTRATE	
	1. CA verification by CA verification Officer (trusted member) 2. Approval procedure for identifying and checking each CA officer. 3. DSC & Video of the approver	
4	**APPLICANT APPROVAL**	
	Login with USERID PIN & OTP – session start	
	Display the user agreement & sign	
	CAs approval of KYC account	
	Applicant generate DSC application form with response code, display & sign	
	CA activate eKYC account -Session end	
	CA enable DSC for download	

	Upon activation of an eKYC account, previously submitted information should only be accessible through the eKYC account.	
	DEMONSTRATE	
	1. Login with two factor authentication by DSC applicant	
	2. eSign on the agreement & option for user to accept or reject	
	3. User see the DSC application form & sign The DSC application form shall mandatorily contain requested DSC details(Class, signature/encryption, validity, Indian etc) Name , address, Photo, PAN/Aadhaar, response code, email etc as in Form C)	
	4. After eKYC account activation, a. upon authenticating (mobile authentication) with a mobile number and OTP, a fresh entry page should be displayed. b. upon authenticating (eKYC account authentication) with a mobile number, PIN and OTP, the user dash board should be displayed	
	5. PIN reset.	
	6. During the session, the input options & CA actions are **NOT** interchangeable between the start and end	
	7. The dash board of the eKYC user	

5. CHECK LIST FOREIGN NATIONAL AUTHENTICATION (PERSONAL/ORGANISATIONAL)

SL	CHECK POINTS	CCA REMARKS
1.	**GENERAL**	
	Select Indian /**Foreign**	
	Select **personal /organisational** (Authorized Signatory / Employee)	
	Select **class/validity**	
	Select **signature**/encryption	
	Select services (token/ support service)	
	KYC Type (**PAN** / **online**)	
	Display Price	
2	**KYC Enrolment FOREIGN NATIONAL (PERSONAL/ORGANISATIONAL)**	
	email OTP authentication – Session start	
	If KYC enrolment page is not called from CA site it should not allow. Link or call to this page not allowed	
	Optionally, display the previously selected **GENERAL** information in an editable form, or provide an option to select general parameters directly here	
	Mobile No: Verify with SMS/DIRECT CALL	
	1. IF PAN AVAILABLE: PAN API (PAN, name, and DoB) - verify Aadhaar linking status & apply state exception order. - No option for editing/changing Name - Option for re-authenticate 2. NAME: ENTRY (IF PAN NOT AVAILABLE)	
	Address – Entry(personal/Official)	
	Email – As used in authentication (non editable)	
	Upload documents (individual / organisational /authorisation)	
	Video verification - option for review- re-verification	
	User ID & PIN	
	Payment & Invoice – through international gateway like PayPal, etc	
	Business Partner (BP) Ref No (optional)	
	Session end	
	DEMONSTRATE	
	1. Name should not be changed in the case of PAN authentication	

	2. If exit during KYC entry, the already entered information should be available after re-authentication using mobile & OTP	
	3. Disposable email check in email verification	
	4. Option for entering user ID & PIN	
	5. Payment: No independent link on the URL other than from within the CA website	
	6. Upload documents, if any	
	7. BP is optional	
	8. During the session, input options can be interchanged freely between the start and end	
	9. The invoice includes only charges for DSC/token/support services.	
3.	**CA VERIFICATION**	
	Verify the completeness and accuracy of the information in accordance with IVG. (individual + organisational +authorisation)	
	Video verification- All photo IDs and video in a single screen -document verification	
	Two level verification	
	Video of the final approver Digital signature of the final Approver.	
	In case of rejection, send a notification to the subscriber to complete it.	
	DEMONSTRATE	
	1. CA verification by CA verification Officer (trusted member) 2. Approval procedure for identifying and checking each CA officer. 3. DSC & Video of the approver 4. Proof of Existence of organisation and its verification details 5. Authorisation from organisation	
4	**APPLICANT APPROVAL**	
	Login with USERID PIN & OTP – session start	
	Display the user agreement & sign	
	CAs approval of KYC account	
	Applicant generate DSC application form with response code, display & sign	
	CA activate eKYC account -Session end	
	CA enable DSC for download	
	Upon activation of an eKYC account, previously submitted information should only be accessible through the eKYC account.	
	DEMONSTRATE	
	1. Login with two factor authentication by DSC applicant	

	2. eSign on the agreement & option for user to accept or reject	
	3. User see the DSC application form & sign The DSC application form shall mandatorily contain requested DSC details (Class, signature/encryption, validity, Indian etc) Name, address, Photo, PAN/Aadhaar, response code, email etc as in Form C)	
	4. After eKYC account activation, a. upon authenticating (mobile authentication) with a mobile number and OTP, a fresh entry page should be displayed. b. upon authenticating (eKYC account authentication) with a mobile number, PIN and OTP, the user dash board should be displayed	
	5. PIN reset.	
	6. During the session, the input options & CA actions are **NOT** interchangeable between the start and end	
	7. The dash board of the eKYC user	

6. ANNEX CHECK LIST ORAGNISATIONAL (AUTHORISED SIGNATORY AND ORGANISATION)

SL	CHECK POINTS	CCA REMARKS
1.	**GENERAL**	
	Select **Indian** /Foreign	
	Select personal /**organisational (Authorized Signatory** / Employee)	
	Select **Class/validity**	
	Select **signature**/encryption	
	Select services(token/ support service)	
	KYC Type (**PAN / Aadhaar -Offline** / online)	
	Display Price	
2	**KYC Enrolment – ORGANISATIONAL (AUTHORISED SIGNATORY AND ORGANISATION)**	
	Mobile OTP authentication – Session start	
	If KYC enrolment page is not called from CA site it should not allow. Link or call to this page not allowed	
	Optionally, display the previously selected general information in an editable form, or provide an option to select general parameters directly here	
	PAN API (PAN, name, and DoB) - verify Aadhaar linking status & apply state exception order. - No option for editing/changing Name - Option for re-authenticate	
	(Optional)Aadhaar: Redirect [start session A] user to a CA page for capturing Aadhaar Number, Biometric , consent, etc - UID - **Back to KYC enrolment page** with response**[end session A]** If Aadhaar eKYC page is not called from KYC enrolment page it should not allow. Link or independent call to this page shall not allowed Display only last four digit of Aadhaar in the KYC page	
	Name as in Aadhaar or PAN as per the verification	
	Address (Office address)	
	Mobile No(Non editable)	
	Email – Verification	
	Upload documents & photo	
	Video verification - option for review- re-verification	
	User ID & PIN	
	Payment & Invoice **OR** Payment RefID [OPTIONAL IF NO DSC IS ISSUED]	
	Business Partner (BP) Ref No (optional)	

	Session end	
	DEMONSTRATE	
	1. Mobile no cannot be changed	
	2. Name as in Aadhaar or PAN	
	3. Address as in Organisation only	
	4. Mobile Number & Name is not editable	
	5. If exit during KYC entry, the already entered information should be available after re-authentication using mobile & OTP	
	6. The option for review- re-verification in video by the applicant	
	7. Disposable email check in email verification	
	8. Option for entering user ID & PIN	
	9. Payment: No independent link on the URL other than from within the CA website	
	10. Upload documents 11. Provision to verify the electronic signature on the electronically signed documents.	
	12. BP is optional	
	13. In case Payment RefID used, the traceability to the details - Invoice can be individual or composite	
	14. During the session, input options can be interchanged freely between the start and end	
	15. The invoice includes only charges for DSC/token/support services.	
3.	**CA VERIFICATION**	
	Verify the completeness and accuracy of the information in accordance with IVG.	
	Video verification- All photo IDs and video in a single screen -document verification	
	Verification -Out of band	
	Two level verification	
	Video of the final approver Digital signature of the final Approver.	
	In case of rejection, send a notification to the subscriber to complete it.	
	DEMONSTRATE	
	1. CA verification by CA verification Officer(trusted member) 2. Approval procedure for identifying and checking each CA officer. 3. DSC & Video of the approver	
4	**APPLICANT APPROVAL**	

	Login with USERID, PIN & OTP – session start	
	Display the user agreement & sign	
	CAs approval of KYC account.	
	Applicant generate DSC application form with response code, display & sign	
	CA activate eKYC account (user/authorised signatory) -Session end	
	CA enable DSC for download or enable eSign (as user & authorised signatory)	
	Upon activation of an eKYC account, previously submitted information should only be accessible through the eKYC account.	
	DEMONSTRATE	
	1. Login with two factor authentication by DSC applicant	
	2. eSign on the agreement & option for user to accept or reject	
	3. User see the DSC application form & sign The DSC application form shall mandatorily contain requested DSC details (Class, signature/encryption, validity, Indian etc), Name, address, Photo, PAN/Aadhaar, response code, email etc as in Form C)	
	4. After eKYC account activation, c. upon authenticating (mobile authentication) with a mobile number and OTP, a fresh entry page should be displayed. d. upon authenticating (eKYC account authentication) with a mobile number, PIN and OTP, the user dash board should be displayed.	
	5. PIN reset.	
	6. During the session, the input options & CA actions are NOT interchangeable between the start and end	
	7. The dash board of the eKYC user and Authorised Signatory	

7. ANNEXURE - CHECK LIST ORAGNISATIONAL PERSON

SL	CHECK POINTS	CCA REMARKS
1.	**GENERAL**	
	Select **Indian** /Foreign	
	Select personal /**organisational (**Authorized Signatory / **Employee**)	
	Select **Class/validity**	
	Select **signature**/encryption	
	Select services (token/ support service)	
	KYC Type (**PAN / Aadhaar -Offline** / online)	
	Display Price	
2	**KYC Enrolment – ORGANISATION (ORAGNISATIONAL PERSON)**	
	Mobile OTP authentication – Session start	
	If KYC enrolment page is not called from CA site it should not allow. Link or call to this page not allowed	
	Optionally, display the previously selected general information in an editable form, or provide an option to select general parameters directly here	
	PAN API (PAN, name, and DoB) - verify Aadhaar linking status & apply state exception order. - No option for editing/changing Name - Option for re-authenticate	
	(Optional)Aadhaar: Redirect [start session A] user to a CA page for capturing Aadhaar Number, Biometric , consent, etc - UID - **Back to KYC enrolment page** with response**[end session A]** If Aadhaar eKYC page is not called from KYC enrolment page it should not allow. Link or independent call to this page shall not allowed Display only last four digit of Aadhaar in the KYC page	
	Name as in Aadhaar or PAN as per the verification	
	Address (Office Address)	
	Mobile No (Non editable)	
	Email – Verification	
	Upload documents & photo	
	Video verification - Option for review- re-verification	
	User ID & PIN	
	Payment & Invoice **OR** Payment RefID	
	Authorised signatory Reference	

	Business Partner(BP) Ref No (optional)	
	Session end	
	DEMONSTRATE	
	1. Mobile no cannot be changed	
	2. Name as in Aadhaar or PAN	
	3. Address as in Organisation only	
	4. Mobile Number & Name is not editable	
	5. If exit during KYC entry, the already entered information should be available after re-authentication using mobile & OTP	
	6. The option for review- re-verification in video by the applicant	
	7. Disposable email check in email verification	
	8. Option for entering user ID & PIN	
	9. Payment: No independent link on the URL other than from within the CA website	
	10. Upload documents 11. Provision to verify the electronic signature on the electronically signed documents.	
	12. BP is optional	
	13. In case Payment RefID used, the traceability to the details - Invoice can be individual or composite	
	14. The presence of authorised signatory reference.	
	15. During the session, input options can be interchanged freely between the start and end	
	16. The invoice includes only charges for DSC/token/support services.	
3	**AUTHORISED SIGNATORY APPROVAL**	
	Login with USERID, PIN & OTP by the Authorised signatory	
	Review the application form of the organisational applicant and approve with token based digital signature or eSign	
	DEMONSTRATE	
	The approval interface and procedure	
	The signature of authorised signatory and its preservation.	
4	**CA VERIFICATION**	
	Verify the completeness and accuracy of the information in accordance with IVG.	
	Video verification- All photo IDs and video in a single screen -document verification	
	Two level verification	
	Video of the final approver	

	Digital signature of the final Approver.	
	In case of rejection, send a notification to the subscriber to complete it.	
	DEMONSTRATE	
	1. CA verification by CA verification Officer (trusted member) 2. Approval procedure for identifying and checking each CA officer. 3. DSC & Video of the approver	
5	**APPLICANT APPROVAL**	
	Login with USERID, PIN & OTP – session start	
	Display the user agreement & sign	
	CAs approval of KYC account.	
	Applicant generate DSC application form with response code, display & sign	
	CA activate eKYC account (user/authorised signatory) -Session end	
	CA enable DSC for download or enable eSign (as user & authorised signatory)	
	Upon activation of an eKYC account, previously submitted information should only be accessible through the eKYC account.	
	DEMONSTRATE	
	1. Login with two factor authentication by DSC applicant	
	2. eSign on the agreement & option for user to accept or reject	
	3. User see the DSC application form & sign The DSC application form shall mandatorily contain requested DSC details (Class, signature/encryption, validity, Indian etc), Name, address, Photo, PAN/Aadhaar, response code, email etc as in Form C)	
	4. After eKYC account activation, a. upon authenticating (mobile authentication) with a mobile number and OTP, a fresh entry page should be displayed. b. upon authenticating (eKYC account authentication) with a mobile number, PIN and OTP, the user dash board should be displayed.	
	5. PIN reset.	
	6. During the session, the input options & CA actions are NOT interchangeable between the start and end	
	7. The dash board of the eKYC user	