Institute for Development and Research in Banking Technology

(Estb. By RBI in 1996)

बैंकिंग प्रौद्योगिकी विकास और अनुसंधान संस्थान

(भारतीय रिजर्व बैंक द्वारा स्थापित - 1996)

Handbook for Organizational Subscribers

Published by : eMudhra Limited, Bengaluru – 562149.
Phone: +91 80 42275300 | Fax: +91 80 42275306 Website: www.emudhra.com

1. Introduction

This document provides a comprehensive user manual for IDRBT users interacting with the Subscriber Portal. It covers every step involved in the subscriber registration, eKYC process, DSC/eSign purchase, and certificate management.

2. Enroll for New User

For new subscribers who do not have an existing account, the 'Enroll for New User' option must be used.

- Clicking this option displays a registration form where the subscriber enters their mobile number and catch. After clicking 'Get OTP', an OTP is sent to the registered mobile number. This OTP must be entered in the provided field to verify the mobile number before proceeding to the next step.
- This step focuses on the mobile number verification process. The subscriber receives a One-Time Password (OTP) via SMS. The OTP must be entered in the field marked 'Mobile OTP'. Clicking the 'Next' button confirms the mobile verification and proceeds to the email registration step.
- After successful mobile OTP verification, the subscriber is prompted to enter their email address. Once entered, an OTP is sent to the email for validation. This is an essential step to confirm the authenticity of the subscriber's email address. Subscriber must click on "Verify Email OTP". After entering the email OTP, the subscriber has to proceed to set their login PIN.
- After both mobile and email OTPs are successfully verified, the subscriber is prompted to complete the remaining registration fields. These include setting a 'Login PIN' and confirming it. Once all fields are filled, clicking the 'Create Account' button completes the registration. A success message will confirm that the account has been created.
- The subscriber will be shown a Subscriber Agreement, click on the link. This document outlines the terms and conditions that govern the use of digital signature services. The subscriber must read the agreement and then click 'Agree & Sign' to accept the terms. This is a mandatory step for using the DSC/eSign services after which they can click on the checkbox.

NOTE: If the subscriber enters an incorrect OTP during enrolment, an **"Invalid OTP"** pop-up message will be displayed. If the subscriber enters an incorrect OTP **three times consecutively**, their account will be **temporarily blocked**.

While registering Email ID, if subscriber is entering incorrect OTP, they will receive a pop-up message as below:

If the subscriber enters an incorrect OTP during enrolment, an **"Invalid OTP"** pop-up message will be displayed. If the subscriber enters an incorrect OTP **three times consecutively**, their account will be **temporarily blocked**.

NOTE: While entering the Login PIN, the subscriber must avoid using simple or easily guessable sequences (for example, 12345678 or 11223344); if such a serial or repetitive PIN is entered.

The system displays a pop-up warning message instructing the subscriber to choose a stronger PIN.

After accepting the Subscriber Agreement, the system confirms the creation of the account. This confirmation ensures that the subscriber's registration and agreement acknowledgement are complete. The subscriber is now allowed to log in using the mobile number and begin the eKYC and DSC/eSign purchase journey.

Once the account is created, a welcome email is sent to the registered email address. This email confirms the registration and includes details such as login ID or further instructions for proceeding. The subscriber should retain this email for future reference.

3. Login

3.1.1. Login using Mobile OTP

- Subscribers can log in to the portal by entering their registered mobile number, captcha and click on 'Get OTP'. OTP will be sent on the registered mobile, verifying the OTP the subscriber can access the portal by clicking the 'Login' button. This method ensures secure access and is applicable for users who have already completed the registration.
- If they enrolled as Individual, they must select Individual radio button.
- If they enrolled as organization, they must select organization radio button.
- If the subscriber is entering wrong OTP they will get a pop up as below,
- After 3 incorrect attempts, there will be a pop-up as below:

- Again after 15 minutes, if the subscriber is entering wrong OTP. If they are entering wrong OTP thrice, the account will be blocked and they will get a pop up as below, they will have to contact administrator to unblock.

3.1.2. Login using eKYC ID & PIN

The subscriber must enter their eKYC ID, PIN, and the displayed captcha, then click Validate PIN. After successful validation, an OTP is sent to the registered mobile number. The subscriber must enter the OTP and click Login to access the portal.

3.2. Dashboard

Upon successful login, the subscriber is redirected to the Dashboard. The Dashboard provides a consolidated view of the account including eKYC status, subscription plans, recent transactions, signed documents, and quick links for performing key activities such as completing eKYC.

3.2.1. Complete eKYC

Before purchasing DSC or initiating eSign transactions, the subscriber must complete the eKYC process. From the Dashboard, the subscriber can click on the 'Complete eKYC' button or navigate through the menu. The eKYC page offers options to select plans and provide identity details such as Aadhaar and PAN.

Step1: Select Plan

- The subscriber needs to select a purchase plan before proceeding with identity verification. The subscriber can choose between different DSC or eSign plans by selecting 'Purchase Plan'.
- After choosing to purchase a DSC or eSign plan, the subscriber can select the desired plan from a dropdown list. Once a plan is selected, the details of the plan will be displayed on screen for review before proceeding to payment.

- After reviewing the plan, the subscriber proceeds to make payment using the available gateways. The subscriber can choose to pay via debit/credit card or net banking. Once the payment method is selected, the subscriber is redirected to the bank portal to complete the transaction.

- After successful payment, a confirmation message is displayed. This confirms that the transaction has been completed and allows the subscriber to proceed with the eKYC process. A receipt or transaction ID may also be generated at this stage.
- A confirmation email containing the invoice for the purchase is sent to the subscriber’s registered email address. This email includes the transaction ID, plan details, and the amount paid for recordkeeping purposes.

Step 2: Organization Details

- If the subscriber has a GSTIN, they should select “Yes”, enter the GSTIN in the GSTIN field, and click Verify GSTIN to validate the number before proceeding.
- Address page will pop up after verification as below, subscriber must select the relevant address
- Once GSTIN is verified successfully, all the details will be fetched automatically
- Subscriber must click on save and proceed after verification.
- If they want to edit GSTIN number, they can click on edit details and change it.

If the subscriber selects” No “for GSTIN in Step 2 – Organization Details, they must manually enter all organization information, including Organization Name, Organization PAN, CIN (if applicable), full address (Address, Street Name, Locality/Colony, Town/Suburb/Village), Country, State, District/City, and Postal Code, and then click Save and Proceed to continue with eKYC process.

If they want to edit any details, they can click on edit details and change it.

Step3: Applicant Details

Step-by-Step Process for eKYC Using Aadhaar (OTP) Method

1. Select eKYC Method

Begin by logging into the portal and choosing your preferred eKYC method.

2. Aadhaar Authentication

- You are redirected to an Aadhaar eKYC user authentication screen.
- Enter your Aadhaar number or VID (Virtual ID), agree to the consent statement, and click SEND OTP.
- An OTP is sent to your Aadhaar-linked mobile. Enter this OTP on the screen to continue.

3. PAN Details Submission

- Once your Aadhaar OTP is successfully verified, proceed to enter your PAN number.

  Full name and DOP will be auto fetched.
- Click Next. The portal verifies your PAN credentials in real time.
- If the PAN number is incorrect, pop up will appear as below.

  To validate the details, click on next, if all the details are correct. Below screen will appear

4. Record Video for IPV (In-Person Verification)

- After successful PAN verification, proceed to the video recording phase.
- The system displays instructions for video recording. Review these instructions carefully. Steps include granting camera access, positioning your face in front of the camera, and recording your answers to prompted questions.
- Record the video as per instructions, preview it if needed, and then submit once satisfied.

After recording, the user can preview the video and either re-record or submit it if satisfied. This submission finalizes the video verification step.

Once submitted, the system processes the video and displays a confirmation message. This means the video has been successfully uploaded.

5. Status Tracking and Confirmation Email

- After the video is uploaded, a status screen will confirm “eKYC Video Submitted Successfully”.
- You’ll also receive an email notification confirming successful video submission and eKYC completion (pending CA review).

6. eKYC Status Update and Forwarding

- The system dashboard indicates completion of Aadhaar and video-based eKYC with the status progressing to “eKYC Completed”.
- Your application is now automatically forwarded to the Certificate Authority (CA) for Level 1 and Level 2 approvals and agreement processes.

Once Aadhaar and video verification are successfully completed, the system displays a success message and the eKYC status is marked as complete. The request is now forwarded to the CA portal for approval at Level 1 and Level 2.

4. Organization Login

- The login page for organization users allows authentication via Mobile Number & OTP. The user enters the mobile number, captcha and OTP to login.
- If they enrolled as Individual, they must select Individual radio button.
- If they enrolled as organization, they must select organization radio button.

4.1. Enroll as Organization User

- New organizations can initiate registration by clicking on 'Enroll for New Organization User'. This opens a form where the organization must select an identifier (such as Organization Name, GSTIN, or PAN) to proceed with account setup.
- When enrolling as an organizer on the eKYC platform, if your organization does not have a GSTIN, you should select the checkbox labelled "This Organization not registered for GST." Once this option is checked, you are allowed to proceed by entering the organization’s PAN number or Organization Name.
- After entering the PAN and providing your mobile number, you will receive an OTP on the given mobile. Enter the OTP in the provided field and click "NEXT" to continue the enrolment process. If you attempt to proceed without GSTIN, the system will explicitly confirm that you can continue with PAN or Organization Name, ensuring that non-GST registered organizations can successfully sign up.

4.2. Enroll using Organization Name

If 'Organization Name' is selected as the identifier, the organization must enter its name and provide supporting details. This option enables entities without GSTIN or PAN to still onboard through a valid identity.

After entering the mobile number, the organization authorized signatory (AS) will receive an OTP for verification. The OTP should be entered in the designated field to confirm mobile ownership and proceed with the registration process. Once the mobile number is verified, the organization must enter a valid email address. An OTP is sent to this email, which must be entered for validation and to continue with the registration.

If the subscriber is entering wrong OTP they will get a pop up as below,

After 3 incorrect attempts, there will be a pop-up as below:

After successful OTP verifications, the organization fills in remaining details such as login PIN and confirms them. Clicking 'Create Account' completes the registration and triggers a confirmation message.

The Authorized signatory must agree to the Subscriber Agreement terms, which govern the use of the platform and digital certificates. The user should read the document carefully and click 'Agree & Sign' to proceed.

Upon successfully signing the agreement, the Authorized signatory 's account is created. The portal displays a success message confirming the account setup and readiness for login.

A confirmation email is sent to the registered email ID containing account activation and next-step instructions. This email serves as an official confirmation of account creation.

4.3. Enroll as Organization PAN

Click on enroll as Organization User

Step 1: Start Enrolment with Organization PAN

- They need to click on the check box "This Organization not registered for "GSTIN" On the subscriber portal, select "Organization PAN" as the enrolment type.
- Enter the organization's PAN number in the designated field.
- Fill in the registered mobile number captcha and request an OTP by clicking "Get OTP."
- Once you receive the mobile OTP, enter it to verify ownership of the entered number.

Step 2: Complete Organization Account Details

- After verifying the mobile number, enter your email address and the OTP received on email for further validation.
- Create a secure login PIN and confirm it in the respective fields.
- Review and accept the terms by checking the box for the Subscriber Agreement.

- Click "CREATE ACCOUNT" to submit and complete the eKYC enrolment for the organization under its PAN.

Step 3: Subscriber Creation Confirmation

- Upon successful account creation, a confirmation popup appears stating, "Subscriber Created Successfully. Click here to Login."

- Click "OK" on the popup, or use the provided login link to access your newly created subscriber account and proceed with certificate-related actions.

4.4. Enroll as Organization GSTIN

Step 1: Start Enrolment

On the IDRBT CA Subscriber Portal login page, click the "ENROLL FOR NEW USER" button to begin the eKYC account creation process. Here you will choose the type of enrolment—"Organization." This step brings up the enrolment form where organizational details must be entered.

Step 2: Enter GST and Mobile Number

- The "Create Your Account" screen prompts for mandatory details.

- Enter your organization’s GSTIN in the GST field.
- Provide the registered mobile number linked with the organization.
- Click “Get OTP” to generate a one-time password for mobile number verification.

Step 3: Enter OTP for Verification

- Once you receive the mobile OTP on your registered number, enter it in the Mobile OTP field. The portal will show a timer confirming OTP validity.
- Click “NEXT” after entering the OTP to proceed with verification and initiate subscriber account setup.

Step 4: Complete Account Details

- Proceed to enter additional account details required for eKYC completion:
- Email ID and verification via an OTP sent to this email.

- Set and confirm your Login PIN to secure account access.

- Review and accept the Subscriber Agreement by ticking the checkbox.

- Click “CREATE ACCOUNT” to finalize your eKYC account creation.
  This step ensures secure multi-factor authentication and compliance for CA subscriber accounts

Step 5: Subscriber Creation Confirmation

- After successfully submitting your details and completing OTP verification, a popup appears stating, "Subscriber Created Successfully. Click here to Login."
-
  Click “OK” button, it will redirect to login page.

4.5. Login

There are two ways of login:

Login using mobile number & OTP

Login using eKYC ID, PIN, Mobile OTP

To log in, the organization user must enter the registered mobile number and click 'Get OTP'. Once the OTP is received, it should be entered along with the captcha code, and then the user can click 'Login' to access the portal.

4.5.1. Login using eKYC ID

The subscriber must enter their eKYC ID, PIN, and the displayed captcha, then click Validate PIN.

When a mobile number is linked to multiple eKYC accounts. The user must select the appropriate organization by clicking the Login button next to the corresponding entry. The list shows details like Organization Name, GSTIN, and PAN to help the user make the correct selection.

4.6. Dashboard

After a successful login, the user is redirected to the dashboard. The dashboard displays important information such as eKYC status, DSC/eSign plan status, and navigation options for certificate and user management.

4.7. Complete Organization eKYC using Organization Name

- To proceed with DSC/eSign, the organization must complete the eKYC process. This can be accessed via the dashboard or left navigation pane by clicking 'Complete eKYC'. It leads to a multi-step form to enter all required organizational information.

- In this step, the organization enters details such as organization name, type, GSTIN or PAN, address, and registration information. All fields must be filled accurately to proceed to the next step.

- After entering and reviewing the details, clicking the 'Next' button saves the organization information. A confirmation message is displayed to ensure the data is recorded successfully.

- This section captures the personal and official details of the authorized signatory. The user must enter information such as PAN number, name, date of birth.

- Once the PAN is entered, the system performs automatic verification with backend systems. If successful, the PAN is marked as verified and the process continues to remaining signatory details.

- The user provides gender, department name of the authorized signatory. All details must be accurate to ensure successful eKYC processing.

- The organization authorized signatory(AS) must upload supporting documents including PAN, address proof, Organization ID card. Each document must meet size and format requirements.

- Once all documents are uploaded, a confirmation message is displayed. Users can also preview the uploaded files before proceeding to video verification.

An email notification is sent to the registered email address confirming the successful upload of documents. This helps in tracking progress and ensuring transparency in the process.

- In this step, the authorized signatory initiates video recording by clicking the 'Continue to Video Recording' button. This step is crucial for validating user presence and identity.

- The signatory clicks 'Start Recording' and reads the displayed statement within the 20-second time limit. This ensures a live, verifiable video submission is made.

- After recording, the user can preview the video and either re-record or submit it if satisfied. This submission finalizes the video verification step.

- Once submitted, the system processes the video and displays a confirmation message. This means the video has been successfully uploaded.

- A confirmation email is sent to the registered email address confirming that the video recording step is complete.

- The organization authorized signatory(AS) now selects the appropriate DSC plan. The available plans are listed for selection before proceeding to payment.

- The user selects 'Purchase DSC', reviews the available options, and selects a plan based on validity and usage.

- Once a plan is selected, the system displays all plan-specific details including duration, price, and features. This helps in ensuring transparency before payment.

- The user is redirected to the payment gateway to make the payment using options like card, net banking, or UPI.

- After successful payment, a confirmation screen is shown. The system registers the transaction and links the selected plan with the organization authorized signatory's (AS) account.

- A mail is sent to the organization authorized signatory's (AS) registered email address with invoice details of the DSC plan purchased.

An additional payment confirmation mail will also be sent containing the transaction ID and summary.

Once all the steps - organization info, documents, video, and payment - are done, the eKYC is marked complete. The request is then forwarded for CA (L1 and L2) approval.

4.8. Complete Organization eKYC using Organization PAN

- To proceed with DSC/eSign, the organization must complete the eKYC process. This can be accessed via the dashboard or left navigation pane by clicking 'Complete Organization eKYC'. It leads to a multi-step form to enter all required organizational information.

- In this step, the organization enters details such as organization name, type, GSTIN or PAN, address, and registration information. All fields must be filled accurately to proceed to the next step.

- After entering and reviewing the details, clicking the 'Next' button saves the organization information. A confirmation message is displayed to ensure the data is recorded successfully.

- This section captures the personal and official details of the authorized signatory. The user must enter information such as PAN number, name, date of birth.

- Once the PAN is entered, the system performs automatic verification with backend systems. If successful, the PAN is marked as verified and the process continues to remaining signatory details.

- If the PAN number is incorrect, pop up will appear as below.
- If the Name given is incorrect, the below pop-up will appear.
- If DOB is not matching, the below pop-up will appear.
- The user provides gender, department name of the authorized signatory. All details must be accurate to ensure successful eKYC processing.
- The organization authorized signatory(AS) must upload supporting documents including PAN, address proof, signatory authorization, and organization registration certificates. Each document must meet size and format requirements.
- Once all documents are uploaded, a confirmation message is displayed. Users can also preview the uploaded files before proceeding to video verification.
- An email notification is sent to the registered email address confirming the successful upload of documents. This helps in tracking progress and ensuring transparency in the process.
- In this step, the authorized signatory initiates video recording by clicking the 'Continue to Video Recording' button. This step is crucial for validating user presence and identity.
- The signatory clicks 'Start Recording' and reads the displayed statement within the 20-second time limit. This ensures a live, verifiable video submission is made.
- After recording, the user can preview the video and either re-record or submit it if satisfied. This submission finalizes the video verification step.
- Once submitted, the system processes the video and displays a confirmation message. This means the video has been successfully uploaded.
- A confirmation email is sent to the registered email address confirming that the video recording step is complete.
- The organization authorized signatory(AS) now selects the appropriate DSC plan. The available plans are listed for selection before proceeding to payment.
- The user selects 'Purchase DSC', reviews the available options, and selects a plan based on validity and usage.

- Once a plan is selected, the system displays all plan-specific details including duration, price, and features. This helps in ensuring transparency before payment.

- The user is redirected to the payment gateway to make the payment using options like card, net banking, or UPI.

- After successful payment, a confirmation screen is shown. The system registers the transaction and links the selected plan with the organization authorized signatory's (AS) account.

- A mail is sent to the organization authorized signatory's (AS) registered email address with invoice details of the DSC plan purchased.

- An additional payment confirmation mail will also be sent containing the transaction ID and summary.

- Once all the steps - organization info, documents, video, and payment - are done, the eKYC is marked complete. The request is then forwarded for CA (L1 and L2) approval.

4.9. Complete Organization eKYC using Organization GSTIN

- To proceed with DSC/eSign, the organization must complete the eKYC process. This can be accessed via the dashboard or left navigation pane by clicking 'Complete Organization eKYC'. It leads to a multi-step form to enter all required organizational information.

- Enter GSTIN and click on proceed, In this step, the Authorized signatory enters details such as organization name, type, GSTIN, Incorporation date, CIN(if available), address will be pre-fetched. All fields must be filled accurately to proceed to the next step.

- After entering and reviewing the details, clicking the 'Next' button saves the organization information. A confirmation message is displayed to ensure the data is recorded successfully.

- This section captures the personal and official details of the authorized signatory. The user must enter information such as PAN number, name, date of birth.

- Once the PAN is entered, the system performs automatic verification with backend systems. If successful, the PAN is marked as verified and the process continues to be remaining signatory details.

- If the PAN number is incorrect, pop up will appear as below.
- If the Name given is incorrect, the below pop-up will appear.

- If DOB is not matching, the below pop-up will appear.

- The user provides gender, department name of the authorized signatory. All details must be accurate to ensure successful eKYC processing.

- The organization authorized signatory(AS) must upload supporting documents including PAN, address proof, signatory authorization, and organization registration certificates. Each document must meet size and format requirements.

- Once all documents are uploaded, a confirmation message is displayed. Users can also preview the uploaded files before proceeding to video verification.

- An email notification is sent to the registered email address confirming the successful upload of documents. This helps in tracking progress and ensuring transparency in the process.

- In this step, the authorized signatory initiates video recording by clicking the 'Continue to Video Recording' button. This step is crucial for validating user presence and identity.

- The signatory clicks 'Start Recording' and reads the displayed statement within the 20-second time limit. This ensures a live, verifiable video submission is made.

- After recording, the user can preview the video and either re-record or submit it if satisfied. This submission finalizes the video verification step.

- Once submitted, the system processes the video and displays a confirmation message. This means the video has been successfully uploaded.

- A confirmation email is sent to the registered email address confirming that the video recording step is complete.

- The organization authorized signatory(AS) now selects the appropriate DSC plan. The available plans are listed for selection before proceeding to payment.

- The user selects 'Purchase DSC', reviews the available options, and selects a plan based on validity and usage.

- Once a plan is selected, the system displays all plan-specific details including duration, price, and features. This helps in ensuring transparency before payment.

- The user is redirected to the payment gateway to make the payment using options like card, net banking, or UPI.

- After successful payment, a confirmation screen is shown. The system registers the transaction and links the selected plan with the organization authorized signatory’s (AS) account.
- A mail is sent to the organization authorized signatory’s (AS) registered email address with invoice details of the DSC plan purchased.

- An additional payment confirmation mail may also be sent containing the transaction ID and summary.
- Once all the steps - organization info, documents, video, and payment - are done, the eKYC is marked complete. The request is then forwarded for CA (L1 and L2) approval.

NOTE: According to organization type, documents needs to be shown. Below id the list of different organization type along with the documents list.

4.10. RA* under the Old System
Changed status under the New Portal.

- ✓ All user/s under the old Registration Authority (RA) system will continue to hold any valid digital certificate issued by IDRBT CA for its validity period.
- ✓ Under the New System “Registration Authority” or “RA” role and definition has changed.

- ✓ In the NEW system an Organisation through its internally Authorised Official (after eKYC on IDRBT CA portal) support the subscriber (individual/s) on demand for enrolment process for Digital Signature Certificate (DSC) to be issued by IDRBT.
- ✓ This system is aimed to enable easy management of digital certificate distribution inside the organisation.

***"Registration Authority" or "RA"** *is an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of applicant's credentials. (Old system definition)*

4.11. Subscriber Agreement

- After CA approval, the authorized signatory must log in again and accept the Subscriber Agreement.
- Clicking **'Agree & Sign'** successfully submits the signed agreement and allows access to DSC application form.
- If the subscriber clicks **'Reject'**, all certificates for the user will be rejected and the enrolment process is terminated. The user must start a new registration if they wish to proceed further.
- The DSC form collects official information such as organization name, common name, and purpose.
- All form fields are auto-filled from eKYC, but must be reviewed. Clicking **'Agree & Sign'** submits the form. A confirmation message appears, and certificate download becomes available.
- If the user clicks **'Reject'**, this DSC application will be rejected. Any existing activated certificate remains active, and if required, the user can purchase a new DSC from the "My Subscription" section.
- The dashboard displays updated status, access to certificates, and subscription actions.

4.12. Manage Certificate

- Certificates are listed here with status. Users can take action like Setup, View, or Download Clicking 'Download' opens a form to enter Application ID and Download PIN for validation that must have been received through mail.
- The details page confirms the request. After entering OTP and PIN, download begins.
- The token type is selected and the token password is entered to install the certificate.
- Once the token is validated, the certificate is downloaded successfully to the device.

Filters under Manage Certificate

- Active: Shows all certificates that are currently valid and usable.
- Pending: Displays certificate requests that are pending for setup.
- Expired: Lists certificates that are no longer valid because their validity period has ended.

- In-Progress: Includes certificates that are currently being processed, either at the applicant or approver stage.
- Rejected: Shows applications that are rejected by CA.
- Revoked: Lists certificates that were previously active but have been intentionally invalidated before their expiry (e.g., due to compromise or policy decisions).
- Suspended: Displays certificates temporarily disabled and not usable until reactivated, pending further review or resolution.

Application ID- Using this option we can search certificate by the ID.

Advance search option

This is the Advance Search feature within the Digital Certificate Details section, which allows users to precisely filter and locate certificate records based on multiple criteria:

- **Search By:**
  You can choose to search certificates by either **"Application ID" or "Common Name"** (the applicant's or organization's name). Enter the relevant search value in the text box.
- **Status:**
  Select the status or statuses you want to filter by (Active, Pending, Expired, In-Progress, Rejected, Revoked, Suspended). Multiple statuses can be selected simultaneously for more comprehensive search results.
- **Include the date range:**
  If you check this option, you can specify a "From" and "To" date using the calendar pickers to narrow results to certificates created, modified, or expiring within the selected timeframe.
- **Controls:**
  - Reset will clear all selected filters and restore the default search view.
  - Search will apply the chosen criteria and display the filtered list of certificate applications matching your inputs.

4.13. Different types of Certificates Set Up & Download Flow

4.13.1.1. System Certificate

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan
Begin the process by selecting your desired DSC plan.
You will see available options such as **"System Certificate - Class 3, 1 Year."**
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference.
Check your order summary, enter all details correctly, and proceed with **"Pay Now."**

Step 4: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode.
Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Step 1: Access the Certificate Setup

Click on the **“Setup”** button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 2: Applicant and Organization Details

Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click **“Proceed”** to continue to the next step of certificate generation.

Step 3: Upload Your CSR File

In this step, upload the Certificate Signing Request (CSR) file by clicking “Choose File.”
About CSR: As per IOG **(Interoperability Guidelines**), a CSR file must be generated by the subscriber. The CSR securely binds identity information and public key for the certificate. Use OpenSSL or your enterprise tool to create this file before uploading. After uploading, click “Validate CSR” to confirm its correctness.

Step 4: Proceed and Edit

When the CSR is validated, you can proceed to the next stage or choose to “Edit” if edits to the CSR or details are required. Confirm successful validation before moving forward.

Step 5: Upload Supporting Documents

Now, upload mandatory supporting documents (in PDF format) for additional identity and compliance proof. Once uploaded, you’ll see options to “Download” and “View” the document for confirmation, ensuring all files are correctly submitted.

Step 6: Video Verification

- If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click “Record Video” to add new verification footage as required by

compliance.
Once video is uploaded, submit for verification.

- The signatory clicks 'Start Recording' and reads the displayed statement within the 20-second time limit. This ensures a live, verifiable video submission is made.
- After recording, the user can preview the video and either re-record or submit it if satisfied. This submission finalizes the video verification step.
- Once submitted, the system processes the video and displays a confirmation message. This means the video has been successfully uploaded

Step 7: Submit for Verification

After completion of document and video uploads, click “Submit for Verification.” A system confirmation popup will indicate successful submission.

Step 8: Monitor Status & CA Approval

Go to the “Manage Certificate” dashboard to check application status. The record will show the current phase (pending, approved, active, etc.).

Once CA approved, they need to do esign.

You’ll be able to download the issued certificate in .cer format from the provided download link.

4.13.1.2. Document Signer Class 3 Certificate

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan

Begin the process by selecting your desired DSC plan.
You will see available options such as "Document Signer - Class 3, 1 Year."
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference.
Check your order summary, enter all details correctly, and proceed with "Pay Now."

Step 4: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode.

Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Step 1: Access the Certificate Setup
Click on the “Setup” button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 2: Applicant and Organization Details
Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click “Proceed” to continue to the next step of certificate generation.

Step 3: Upload Your CSR File
In this step, upload the Certificate Signing Request (CSR) file by clicking “Choose File.”
About CSR: As per IOG (Interoperability Guidelines), a CSR file must be generated by the subscriber. The CSR securely binds identity information and public key for the certificate. Use OpenSSL or your enterprise tool to create this file before uploading. After uploading, click “Validate CSR” to confirm its correctness.

5. Step 4: Proceed and Edit

When the CSR is validated, you can proceed to the next stage or choose to “Edit” if edits to the CSR or details are required. Confirm successful validation before moving forward.

6. Step 5: Upload Supporting Documents

Now, upload mandatory supporting documents (**in PDF format**) for additional identity and compliance proof. Once uploaded, you’ll see options to “Download” and “View” the document for confirmation, ensuring all files are correctly submitted.

7. Step 6: Video Verification

- If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click “Record Video” to add new verification footage as required by compliance.
  Once video is uploaded, submit for verification.

- The signatory clicks 'Start Recording' and reads the displayed statement within the 20-second time limit. This ensures a live, verifiable video submission is made.
- After recording, the user can preview the video and either re-record or submit it if satisfied. This submission finalizes the video verification step.

- Once submitted, the system processes the video and displays a confirmation message. This means the video has been successfully uploaded.

8. Step 7: Submit for Verification

After completion of document and video uploads, click “Submit for Verification.” A system confirmation popup will indicate successful submission.

9. Step 8: Monitor Status & CA Approval

Go to the “Manage Certificate” dashboard to check application status. The record will show the current phase (pending, approved, active, etc.).
Once CA approved, they need to do esign.

You’ll be able to download the issued certificate in .cer format from the provided download link.

9.1.1.1. Signature Class 3 Certificate

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan
Begin the process by selecting your desired DSC plan.
You will see available options such as "Signature - Class 3"
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference.
Check your order summary, enter all details correctly, and proceed with "Pay Now."

Step 4: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode.

Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Step 1: Access the Certificate Setup

Click on the “Setup” button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 2: Applicant and Organization Details

Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click “Proceed” to continue to the next step of certificate generation.

Step 3: Upload Supporting Documents

Now, upload mandatory supporting documents (in PDF format) for additional identity and compliance proof. Once uploaded, you’ll see options to “Download” and “View” the document for confirmation, ensuring all files are correctly submitted.

Step 4: Video Verification

If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click “Record Video” to add new verification footage as required by compliance.
Once video is uploaded, submit for verification.

The signatory clicks 'Start Recording' and reads the displayed statement within the 20-second time limit. This ensures a live, verifiable video submission is made.

After recording, the user can preview the video and either re-record or submit it if satisfied. This submission finalizes the video verification step.

Once submitted, the system processes the video and displays a confirmation message. This means the video has been successfully uploaded

Step 5: Submit for Verification

After completion of document and video uploads, click “Submit for Verification.” A system confirmation popup will indicate successful submission.

Step 6: Monitor Status & CA Approval

Go to the “Manage Certificate” dashboard to check application status. The record will show the current phase (pending, approved, active, etc.).

Once CA approved, they need to do esign.

Clicking 'Download' opens a form to enter Application ID and Download PIN for validation that must have been received through mail.

The details page confirms the request. After entering OTP and PIN, download begins.

The token type is selected and the token password is entered to install the certificate.

Once the token is validated, the certificate is downloaded successfully to the device.

9.1.1.2. Document Signer Class 2 Certificate

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan

Begin the process by selecting your desired DSC plan.
You will see available options such as "Document Signer - Class 2 "
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference.
Check your order summary, enter all details correctly, and proceed with "Pay Now."

Step 5: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode.
Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Step 1: Access the Certificate Setup

Click on the “Setup” button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 2: Applicant and Organization Details

Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click “Proceed” to continue to the next step of certificate generation.

Step 5: Upload Supporting Documents

Now, upload mandatory supporting documents (in PDF format) for additional identity and compliance proof. Once uploaded, you’ll see options to “Download” and “View” the document for confirmation, ensuring all files are correctly submitted.

Step 6: Video Verification

- If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click “Record Video” to add new verification footage as required by compliance.
  Once video is uploaded, submit for verification.

- The signatory clicks 'Start Recording' and reads the displayed statement within the 20-second time limit. This ensures a live, verifiable video submission is made.

- After recording, the user can preview the video and either re-record or submit it if satisfied. This submission finalizes the video verification step.
- Once submitted, the system processes the video and displays a confirmation message. This means the video has been successfully uploaded

Step 7: Submit for Verification

After completion of document and video uploads, click “Submit for Verification.” A system confirmation popup will indicate successful submission.

Step 8: Monitor Status & CA Approval

- Go to the “Manage Certificate” dashboard to check application status. The record will show the current phase (pending, approved, active, etc.).
- Once CA approved, they need to esign.
- They will receive an email with application ID and download PIN from which they can download the certificate. To download the certificate, navigate to My certificate and click on download.
- Click on proceed and enter the Application ID and Download PIN.
- For document signer there are two options of download type, they can select “Save as PFX or Token”
- If they select PFX, below screen will appear
- Click on agree & download
- They must select where the pfx file needs to be downloaded and they can click on selection done

For pfx : it will be downloaded in the selected path. If download type selected is” Token” Certificate will be downloaded in the token.

9.2. Revoke Certificate

- Once the certificate got downloaded, they can click on view button. Under which they will be getting revoke certification option.

- Click on proceed, to revoke the certificate. Authorized Signatory or Applicant has to enter revocation reason from the list

- If unspecified has been selected, they will have to enter the remarks and then click on submit

- Once submitted successfully, they will be getting the below screen under manage certificate “view option where they can see the status as “Revoke certificate request initiated”.

- After this step, the request will land into CA Portal for approval.
- Once CA will approve the request, the status of certificate will be changed to revoked.

9.3. Suspend Certificate

- Once the certificate got downloaded, they can click on view button. Under which they will be getting suspend certification option. If the certification needs to be suspended for a particular time period, the Authorized Signatory or applicant can go for suspend certificate option.

- Click on Proceed to suspend the certificate. Enter the suspend reason and submit it.
- Once submitted successfully, they can see the status of suspension initiation request
- Once approved by CA, the suspended certificate can be seen under manage certificate tab.

9.4. Activation Certificate

Suspended certificates can only raise a activation request

Click on view button, to initiate activation request for the certificate. Click on activation in the below screen - Enter the activation reason and click on submit

Once submitted, they can see the status under manage certificate section. Click on view button. Once the CA approved, the certificate will be activated

9.5. Reissue Certificate

After downloading the certificate, if the subscriber faces any issue with the certificate then they can reissue the certificate.

Click on view bottom. Once clicked in proceed, New application ID will be generated. After this, the new application will land into CA portal for approval.

Click on submit for verification

Once approval is done, they must esign and download the certificate. After downloading the certificate, the old application will automatically revoke and the new one can be used.

9.6. My Subscription

To purchase eSign or DSC credits, the authorized user goes to 'My Subscription' and selects 'Purchase eSign' or Purchase DSC. The available plans are displayed with validity and usage details.

9.7. Purchase eSign

Once the payment is completed successfully, a confirmation message is shown and the credits are applied to the account.

9.8. Upload & eSign

- Navigate to 'Upload & Sign' to upload the PDF that needs to be digitally signed using eSign credits.
- The uploaded document is previewed before proceeding. The user confirms and continues with eSign placement.
- The document proceeds to signature settings where signing details are entered.

- User inputs name, reason for signing, and other metadata. The eSign appearance can also be configured here.
- Saving the signature settings leads to the eKYC-based verification screen to authorize the signing.
- The user enters their eKYC ID and PIN as an authentication step.
- An OTP is sent to the registered mobile. It must be entered to complete the eSign operation. Once OTP is verified, the document is digitally signed and a success message is displayed.

9.9. eSign Transactions

The signed documents are listed here along with timestamps and status. Download option is available.

9.10. Purchase DSC Plan

- Click on the "Purchase DSC" button from the dashboard or the "My Subscription" section.
- Select the desired DSC Plan suitable for the organization (e.g., Signature - Class 3, 2 Years).
- Review the selected plan details (name, validity, price with GST breakdown).
- Click Next to proceed to payment options and choose the preferred payment method (e.g., SBIePay, net banking, or credit card).
- Click Continue to initiate and complete the online payment.
- Once the transaction is successful, a confirmation page will display your transaction details.
- You can check all purchased certificates and available balances anytime under the "My Subscription" section.

9.10.1. View and Manage Purchased Certificates

- After purchase, navigate to "Manage Certificate" to see all certificate applications, their details, and status (Pending, Active, etc.).
- Every certificate applied or purchased for your organization will be listed here with its Application ID, status, and action buttons.

9.10.2. Complete Certificate Setup (Authorized Signatory)

- The authorized signatory (i.e., the organization admin or designated person) must click "Setup" next to the relevant certificate under "Manage Certificate".
- All organization and applicant details (such as name, organization unit, serial number, company address, etc.) will be auto-fetched into the setup form.
- Carefully review auto-filled details for accuracy and enter/complete any required organizational fields such as department, email, or updated address if required.
- Click Proceed.

9.10.3. Upload Organizational Documents

- Upload the necessary documents for organization verification (such as ID Card and , Authorization Signatory Letter (format) as PDF file.

(To be printed on Organisation Official Letter Head)

Authorized signatory letter to IDRBT CA for eSign/DSC
(To be submitted to IDRBT CA by Authorized Signatory)

The Project -in-Charge
IDRBT Certifying Authority,
Road No 1, Castle Road,
Masab Tank,
Hyderabad – 500057. Dated:

I, (………) as Head of Organisation/Department of the (------……………………………-……………….-------), have understood the requirements of eSign/DSC enrolments under provisions of the extant Information Technology Act, and will authorize the employees in line with these requirements. I have enclosed my ID card issued by the competent authority of the organization.

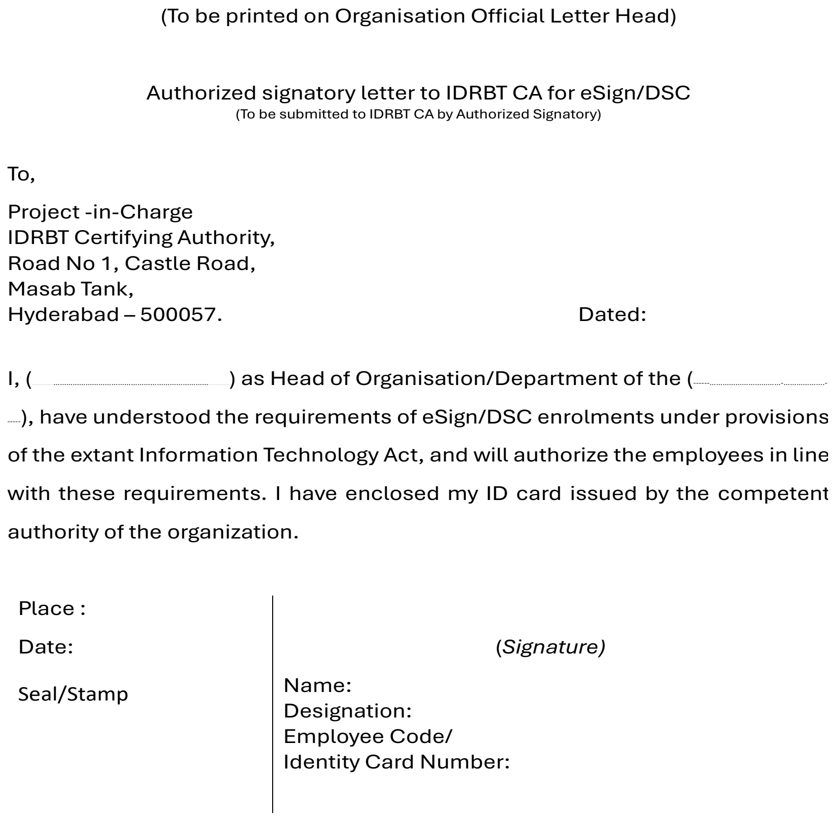
Place :

Date:

Seal/Stamp

(Signature)

Name:
Designation:
Employee Code/
Identity Card Number:



(To be printed on Organisation Official Letter Head)

Authorized signatory letter to IDRBT CA for eSign/DSC
(To be submitted to IDRBT CA by Authorized Signatory)

To,

Project -in-Charge
IDRBT Certifying Authority,
Road No 1, Castle Road,
Masab Tank,
Hyderabad – 500057. Dated:

I, (………………………) as Head of Organisation/Department of the (…………………………), have understood the requirements of eSign/DSC enrolments under provisions of the extant Information Technology Act, and will authorize the employees in line with these requirements. I have enclosed my ID card issued by the competent authority of the organization.

Place :	
Date:	*(Signature)*
Seal/Stamp	Name: Designation: Employee Code/ Identity Card Number:

- Then The authorized person complete and submit the video as prompted.

Proceed to Video Recording for Verification:
Once the documents are verified, you will be prompted to complete the video recording step for verification. Click Continue to Video Recording and follow the instructions to record and submit your verification video.

Status Tracking and Confirmation Email:

- After the video is uploaded, a status screen will confirm “eKYC Video Submitted Successfully”.

9.10.4. Submit for CA Verification

- After uploading documents and/or completing video verification, click the "Submit for Verification" button.
- A confirmation popup will indicate successful setup completion.

9.11. Manage Organization Users

- The Authorized Signatory can view and manage all applicants under the organization from this tab. To begin, the Authorized Signatory must create an applicant by clicking the Create User option. The applicant then completes the eKYC process and receives a confirmation email upon completion. After this, the request appears under the Manage Organization Users tab for the Authorized Signatory's approval.

- For approval, the Authorized Signatory must possess a signature certificate in the token. Using this certificate, they can approve the applicant's request. Once approved, the Authorized Signatory can assign the relevant plan to the applicant. After this step, the applicant's eKYC request is forwarded to the CA portal for final approval.
- New applicants can be created by filling out user-specific fields like email, and mobile number.
- A confirmation message is displayed and the applicant appears in the list of pending users.
- The applicant will receive a mail where they have to complete eKYC process by entering PAN details and completing video recording process. The signatory clicks 'Process' and reviews the applicant details for approval.
- Applicant will receive a mail, and they have to complete ekyc process. After completion of ekyc process it will the application will land under manage organization users, where authorized signatory has to approve it.
- This opens the complete form submitted by the applicant for review.
- If all details are valid, the signatory approves the applicant profile.
- The signatory can assign DSC plans to applicants for their certificate processing.
- The system links the chosen plan with the applicant profile for further processing.
- The applicant selects the assigned DSC plan and proceeds to make payment or complete the process.
- The authorized signatory(AS) completes payment through available gateways and receives confirmation on success. There are two ways of payment
- 1)Generate Payment Link
- 2)Pay now
- On clicking on generate payment link, the below screen will appear from where they can send the payment link.
- If they click on pay now, the below screen will appear.

A success screen appears and the applicant is ready to begin eKYC.

9.12. Applicant account creation

Applicant completes account setup by entering mobile number & captcha followed by OTP verification.

Applicant needs to enter email ID, and they have to click on get OTP.Once they receive OTP , they need to enter it and get verified.

Successful account creation confirmation is displayed and applicant can now log in.

9.12.1. Dashboard

Dashboard displays eKYC status and next steps like completing eKYC or signing the agreement.

9.12.2. Complete Organization eKYC

- Applicant completes eKYC by entering PAN, uploading documents, and recording video.
- PAN details are entered and verified with backend validation.
- Applicant uploads PAN copy and other required documents in the required format.
- Applicant records a video reading the shown code for identity verification. According to the type of organization they have to show the documents while recording the verification video.
- Once the video is submitted, confirmation is displayed and request is forwarded to signatory for approval. Dashboard updates status of eKYC verification and applicant actions.
- Applicant must agree to the Subscriber Agreement terms to continue.
- If the subscriber clicks 'Reject', all certificates for the user will be rejected and the enrollment process is terminated. The user must start a new registration if they wish to proceed further.
- Confirmation appears and applicant is shown DSC application form.

9.12.3. DSC Application Form

Applicant reviews auto-filled DSC form fields.

Form is submitted after applicant agrees and signs digitally. Updated dashboard shows next actions such as certificate download or purchase.

If the user clicks 'Reject', this DSC application will be rejected. Any existing activated certificate remains active, and if required, the user can purchase a new DSC from the "My Subscription" section.

9.12.4. Manage Certificate

Applicant can download DSC after CA approval using this section.

Download requires Application ID, Download PIN, OTP, and token password.

Displays issued certificate metadata and subject information.

OTP is requested before final download step. OTP is verified to continue to token setup. Token password is entered and token validated for certificate installation. Certificate download completes successfully and is stored securely in token.

9.13. Different types of Certificates Set Up & Download Flow

9.13.1.1. System Certificate

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan

Begin the process by selecting your desired DSC plan.
You will see available options such as "System Certificate - Class 3, 1 Year."
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference. Check your order summary, enter all details correctly, and proceed with "Pay Now."

Step 5: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode. Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Step 1: Access the Certificate Setup

Click on the “Setup” button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 2: Applicant and Organization Details

Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click “Proceed” to continue to the next step of certificate generation.

Step 3: Upload Your CSR File

In this step, upload the Certificate Signing Request (CSR) file by clicking “Choose File.”
About CSR: As per IOG (Interoperability Guidelines), a CSR file must be generated by the subscriber. The CSR securely binds identity information and public key for the certificate. Use OpenSSL or your enterprise tool to create this file before uploading. After uploading, click “Validate CSR” to confirm its correctness.

Step 4: Proceed and Edit

When the CSR is validated, you can proceed to the next stage or choose to “Edit” if edits to the CSR or details are required. Confirm successful validation before moving forward.

Step 5: Upload Supporting Documents

Now, upload mandatory supporting documents (in PDF format) for additional identity and compliance proof. Once uploaded, you’ll see options to “Download” and “View” the document for confirmation, ensuring all files are correctly submitted.

Step 6: Video Verification

If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click “Record Video” to add new verification footage as required by compliance. Once video is uploaded, submit for verification.

Step 7: Submit for Verification

After completion of document and video uploads, click “Submit for Verification.” A system confirmation popup will indicate successful submission.

Step 8: Monitor Status & CA Approval

Go to the “Manage Certificate” dashboard to check application status. The record will show the current phase (pending, approved, active, etc.).

Once CA approved, they need to do esign. Once DSC is signed, they can download .cer file from the download link

9.13.1.2. Document Signer Class 3 Certificate

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan

Begin the process by selecting your desired DSC plan.
You will see available options such as "Document Signer - Class 3, 1 Year."
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference.
Check your order summary, enter all details correctly, and proceed with "Pay Now."

Step 5: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode.
Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Step 1: Access the Certificate Setup

Click on the “Setup” button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 2: Applicant and Organization Details

Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click “Proceed” to continue to the next step of certificate generation.

Step 3: Upload Your CSR File

In this step, upload the Certificate Signing Request (CSR) file by clicking “Choose File.”
About CSR: As per IOG (Interoperability Guidelines), a CSR file must be generated by the subscriber. The CSR securely binds identity information and public key for the certificate. Use OpenSSL or your enterprise tool to create this file before uploading. After uploading, click “Validate CSR” to confirm its correctness.

Step 4: Proceed and Edit

When the CSR is validated, you can proceed to the next stage or choose to “Edit” if edits to the CSR or details are required. Confirm successful validation before moving forward.

Step 5: Upload Supporting Documents

Now, upload mandatory supporting documents (in PDF format) for additional identity and compliance proof. Once uploaded, you'll see options to "Download" and "View" the document for confirmation, ensuring all files are correctly submitted.

Step 6: Video Verification

If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click "Record Video" to add new verification footage as required by compliance.
Once video is uploaded, submit for verification.

Step 7: Submit for Verification

After completion of document and video uploads, click "Submit for Verification." A system confirmation popup will indicate successful submission.

Step 8: Monitor Status & CA Approval

Go to the "Manage Certificate" dashboard to check application status. The record will show the current phase (pending, approved, active, etc.).

Once CA approved, they need to do esign.
Once DSC is signed, they can download .cer file from the download link.

9.13.1.3. Signature Class 3 Certificate

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan

Begin the process by selecting your desired DSC plan.
You will see available options such as "Signature - Class 3"
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference. Check your order summary, enter all details correctly, and proceed with "Pay Now."

Step 5: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode.
Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Step 1: Access the Certificate Setup

Click on the "Setup" button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 2: Applicant and Organization Details

Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click "Proceed" to continue to the next step of certificate generation.

Step 3: Upload Supporting Documents

Now, upload mandatory supporting documents (in PDF format) for additional identity and compliance proof. Once uploaded, you'll see options to "Download" and "View" the document for confirmation, ensuring all files are correctly submitted.

Step 4: Video Verification

If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click "Record Video" to add new verification footage as required by compliance.
Once video is uploaded, submit for verification.

Step 5: Submit for Verification

After completion of document and video uploads, click "Submit for Verification." A system confirmation popup will indicate successful submission.

Step 6: Monitor Status & CA Approval

Go to the "My Certificate" dashboard to check application status. The record will show the current phase (pending, approved, active, etc.). Once your application lands in the CA portal and receives the CA's signature, you'll be able to download the issued certificate in .cer format from the provided download link.

Once CA approved, they need to do esign.

Clicking 'Download' opens a form to enter Application ID and Download PIN for validation that must have been received through mail.

The details page confirms the request. After entering OTP and PIN, download begins.

The token type is selected and the token password is entered to install the certificate.

Once the token is validated, the certificate is downloaded successfully to the device.

9.13.1.4. Document Signer Class 2 Certificate

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan

Begin the process by selecting your desired DSC plan.
You will see available options such as "Document Signer - Class 2 "
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference.
Check your order summary, enter all details correctly, and proceed with "Pay Now."

Step 5: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode.
Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Step 1: Access the Certificate Setup

Click on the “Setup” button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 2: Applicant and Organization Details

Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click “Proceed” to continue to the next step of certificate generation.

Step 5: Upload Supporting Documents

Now, upload mandatory supporting documents (in PDF format) for additional identity and compliance proof. Once uploaded, you’ll see options to “Download” and “View” the document for confirmation, ensuring all files are correctly submitted.

Step 6: Video Verification

If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click “Record Video” to add new verification footage as required by compliance.
Once video is uploaded, submit for verification.

Step 7: Submit for Verification

After completion of document and video uploads, click “Submit for Verification.” A system confirmation popup will indicate successful submission.

Step 8: Monitor Status & CA Approval

Go to the “Manage Certificate” dashboard to check application status. The record will show the current phase (pending, approved, active, etc.).
Once CA approved, they need to do esign.
They will receive an email with application ID and download PIN from which they can download the certificate. To download the certificate, navigate to My certificate and click on download

- Click on proceed and enter the Application ID and Download PIN

- For document signer there are two options of download type, they can select “Save as PFX or Token”
- If they select PFX, the screen below will appear
- Click on agree & download.
- They have to select where the pfx file needs to be downloaded and they can click on selection done
- For pfx it will be downloaded in the selected path.
- If they select download type as “Token”
- Certificate will be downloaded in the token

9.13.1.5. Organization Combo (Encryption + Signature) - Class 3

Purchase Digital Certificate Workflow

Step 1: Select the Certificate Plan

Begin the process by selecting your desired DSC plan.
You will see available options such as " Organization Combo (Encryption + Signature) - Class 3"
Review the plan details including validity, cost, and GST breakdown, then click "Next" to continue.

Step 2: Choose Payment Option

You are taken to a payment selection page.
Choose your payment option (for example, "SBIePay"), then click "Continue" to proceed.

Step 3: Enter Payment Details

Fill out payment information such as card details or choose net banking/branch payment as per your preference.
Check your order summary, enter all details correctly, and proceed with "Pay Now.

Step 5: Transaction Success Confirmation

A confirmation screen is displayed with a green tick, showing your transaction ID, amount paid, and payment mode.
Click the provided link to manage your certificate or continue with the next steps in the issuance process.

Access the Certificate Setup

Click on the “Setup” button beside the pending system certificate application in your digital certificate details list. This opens the setup workflow, where key certificate and applicant details will be prefilled from your eKYC records. Carefully check all the auto-fetched information before you proceed to the next stage.

Step 1: Applicant and Organization Details

Review the applicant details, organization unit, contact, address, and other fields pre-filled from the eKYC system. If all information is correct, click “Proceed” to continue to the next step of certificate generation.

Step 3: Upload Supporting Documents

Now, upload mandatory supporting documents (in PDF format) for additional identity and compliance proof. Once uploaded, you'll see options to "Download" and "View" the document for confirmation, ensuring all files are correctly submitted.

Video Verification

If eKYC approval was granted within 48 hours previously, video verification may be auto-fetched; otherwise, click "Record Video" to add new verification footage as required by compliance.
Once video is uploaded, submit for verification

Step 4: Submit for Verification

After completion of document and video uploads, click "Submit for Verification." A system confirmation popup will indicate successful submission.

Step 5: Monitor Status & CA Approval

Go to the "Manage Certificate" dashboard to check application status. The record will show the current phase (pending, approved, active, etc.).
Once CA approved, they need to do esign.

9.13.2. My Subscription

Applicant can purchase eSign or DSC credits from 'My Subscription' for document signing.

9.13.2.1. Purchase eSign

eSign plan payment is completed and credits reflected in account.

9.13.2.2. Upload & eSign

Applicant uploads document and begins eSign flow. PDF preview is available before proceeding to eSign. Applicant moves to signature configuration. Signature name, position, and purpose are entered here. Saves configuration and begins eKYC login prompt. eKYC ID and PIN are entered for verification.

Document is signed and success message displayed.

After clicking on download button, it will be downloaded as a zip file in downloads section.

After extracting the zip folder, they can open the signed document PDF file as below.

9.13.2.3. eSign Transaction

Shows list of eSigned documents with options to download.

Downloading esign document and view signature should be mentioned

9.13.2.4. Purchase DSC

- Click on the "Purchase DSC" button from the dashboard or the "My Subscription" section.
- Select the desired DSC Plan suitable for the organization (e.g., Signature - Class 3, 2 Years).
- Review the selected plan details (name, validity, price with GST breakdown).
- Click Next to proceed to payment options and choose the preferred payment method (e.g., SBlePay, net banking, or credit card).
- Click Continue to initiate and complete the online payment.
- Once the transaction is successful, a confirmation page will display your transaction details.

9.13.2.5. Applicant Certificate Setup

In the "Manage Certificate" section, locate the application listed with status "Pending" and click the Setup button next to it.

- Confirm that Organization Name & all contact details accurately match those in official records.

1. Proceed to Validation Documents

- Scroll down to the "Validation Documents" section.
- Upload the mandatory supporting document by clicking "Browse"/"Choose File," selecting the file, and then clicking Upload.
- If required for the application type, perform video verification by clicking "Record Video" and following the on-screen instructions to complete and submit the verification.

2. Final Review and Submission

- Check that all required document uploads (and video, if needed) show status as "Completed."
- Recheck the top sections for accuracy and completeness of all entered details.
- Click Submit for Verification.

3. Confirmation

- Upon successful submission, a message such as "Setup completed successfully" will be displayed, confirming that the setup phase is done. Click OK on the confirmation popup.

4. Next Steps

- The request now goes to the Certifying Authority (CA) for verification and approval. The applicant may monitor status in the "Manage Certificate" list and await further notification for approval or next actions.