

**CENTRAL REGISTRY OF SECURITISATION ASSET
RECONSTRUCTION AND SECURITY INTEREST OF INDIA
(CERSAI)**

CENTRAL KYC REGISTRY OPERATING GUIDELINES 2016

Version 1.1

The Government of India vide their Notification dated November 26, 2015 authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), set up under sub-section (1) of Section 20 of the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 (54 of 2002), to act as and to perform the functions of the Central KYC Records Registry under the said rules, including receiving, storing, safeguarding and retrieving the KYC records in digital form of a “client”, as defined in clause (ha) of sub-section (1) of Section 2 of the Prevention of Money-Laundering Act, 2002. The Central Government have also amended the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 vide Notification dated 7th July, 2015 for the purpose of establishment of Central KYC Registry. As per Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2015, Rule 9 (1A), every reporting entity shall within three days after the commencement of an account-based relationship with a client, file the electronic copy of the client’s KYC records with the Central KYC Registry.

The Operating Guidelines in the regard are as under:

I. Definitions

In these guidelines, unless the context otherwise requires, the terms defined herein shall bear the meanings assigned to them below –

- a) “Act” means the Prevention of Money Laundering Act, 2002.
- b) “Rules” means Prevention of Money Laundering (Maintenance of Records) Rules, 2005.
- c) “Central KYC Records Registry” (CKYCR) means an entity defined under 2(1) (aa) of the Rules.

- d) "Reporting Entity" means an entity defined under sub-section (wa) of section 2 of the Act.
- e) "Customer" means a client as defined under sub-section (ha) of sub-section 2 of the Act.
- f) "KYC" means the due diligence procedure prescribed by the regulator for identifying and verifying the proof of address, proof of identity and compliance with rules, regulations, guidelines and circulars issued by the regulator or any other statutory authority under the Act from time to time.
- g) "KYC identifier" means a unique identifier for the customer generated by the Central KYC Registry and notified to the reporting entities.
- h) "Operating Guidelines" means operating instructions made by the Central KYC Registry in co-ordination with the regulator/s.

All other words and expressions used but not defined in these guidelines shall have the same meaning as have been assigned to them under the Act or the Prevention of Money laundering (Maintenance of Records) Rules, 2005 or any statutory modification or re-enactment thereto, as the case may be.

II. Functions and Obligations of Central KYC Registry

The Central KYC Registry shall have the following functions and obligations:

- a) Shall have a secure electronic connectivity with the registered reporting entities. The web address of Central KYC Registry portal is <https://www.ckycindia.in>
- b) Shall have a secure data transmission link with the ID issuing authorities wherever feasible and use such electronic data, as permitted, and preserve it with the Central KYC Registry.
- c) Shall be responsible for electronically (i) storing (ii) safeguarding and (iii) retrieving the Know Your Customer (KYC) records and making such records available online to reporting entities or Director.

- d) Information updated about a customer shall be disseminated on request by Central KYC Registry to any reporting entity that avail the services of the Central KYC Registry in respect of the customer.
- e) The services of the Central KYC Registry will be available on payment of prescribed fee, in advance.
- f) Shall process the KYC records received from a reporting entity for de-duplication and issue a unique KYC Identifier for each client to the reporting entity.
- g) Ensure that the integrity of the electronic systems for records is maintained and accessible at all material times.
- h) Take all precautions necessary to ensure that the electronic Know Your Customer (KYC) records are not lost, destroyed or tampered with and that sufficient back up of electronic records is available at all times at a different place.
- i) Take all reasonable measures to prevent unauthorized access to its KYC database.

III. Functions and obligations of the reporting entity

The reporting entity shall have the following functions and obligations:

- a) Reporting entities shall be required to register with the Central KYC Registry in accordance with the processes and instructions issued.
- b) While commencing an account based relationship, reporting entity shall verify the identity of the customer and perform the initial due diligence of the customer.
- c) Where a customer submits a KYC Identifier to a reporting entity, then such reporting entity shall download the KYC records from the Central KYC Registry by using the KYC Identifier and shall not require a customer to submit the documents again unless

- i) There is a change in the information of the customer as existing in the records of Central KYC Registry.
- ii) The current address of the client is required to be verified.
- iii) The reporting entity considers it necessary in order to verify the identity or address of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.
- d) The reporting entity shall not use the KYC data of a customer obtained from the Central KYC Registry for purposes other than verifying the identify or address of the client and shall not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or by the Regulator or by the Director.
- e) The reporting entity which performed the last KYC verification or sent updated information in respect of a client shall be responsible for verifying the authenticity of the identity or address of the client.

The prescribed fee is payable by the reporting entity for each type of transaction and Central KYC Registry will collect such fees from the reporting entities, in advance.

IV. Operating Guidelines to the Reporting Entities

- a) Central KYC Registry application can be accessed by registered/authorised institutions or other notified institutions under the Prevention of Money Laundering Act or rules framed by the Government of India or any Regulator (RBI, SEBI, IRDA and PFRDA) thereunder.
- b) Every reporting entity has to register itself on the Central KYC Registry portal (<https://www.ckycindia.in>) with 2 Primary Users who in turn can create more users (makers and checkers).

A. Registration

Registration process entails the following:

- i. Entry of the requisite details on the registration screen by the Nodal Officer/Authorised Signatory of the reporting entity and online submission of the same.
- ii. Upon submission, reference ID will be generated and an email shall be sent to Nodal Officer/Authorised Signatory's registered email ID. Reporting entity can check the current registration status on the CKYC Portal by the reference number generated.
- iii. Duly signed form along with following supporting documents shall be sent to Central KYC Registry:
 - Duly Signed institution registration form
 - Regulator License/Certificate/Notification
 - PAN Card of the entity
 - Corporate Identification Number (in case regulator issues multiple licenses to an entity)
 - Registration Certificate (In case of Co-operative Banks/societies)
 - Authorization letter by Competent Authority for Admin users
 - Certified copy of photo identity card of the Admin users issued by the institution
 - Certified copy of the proof of the identity of the Admin users

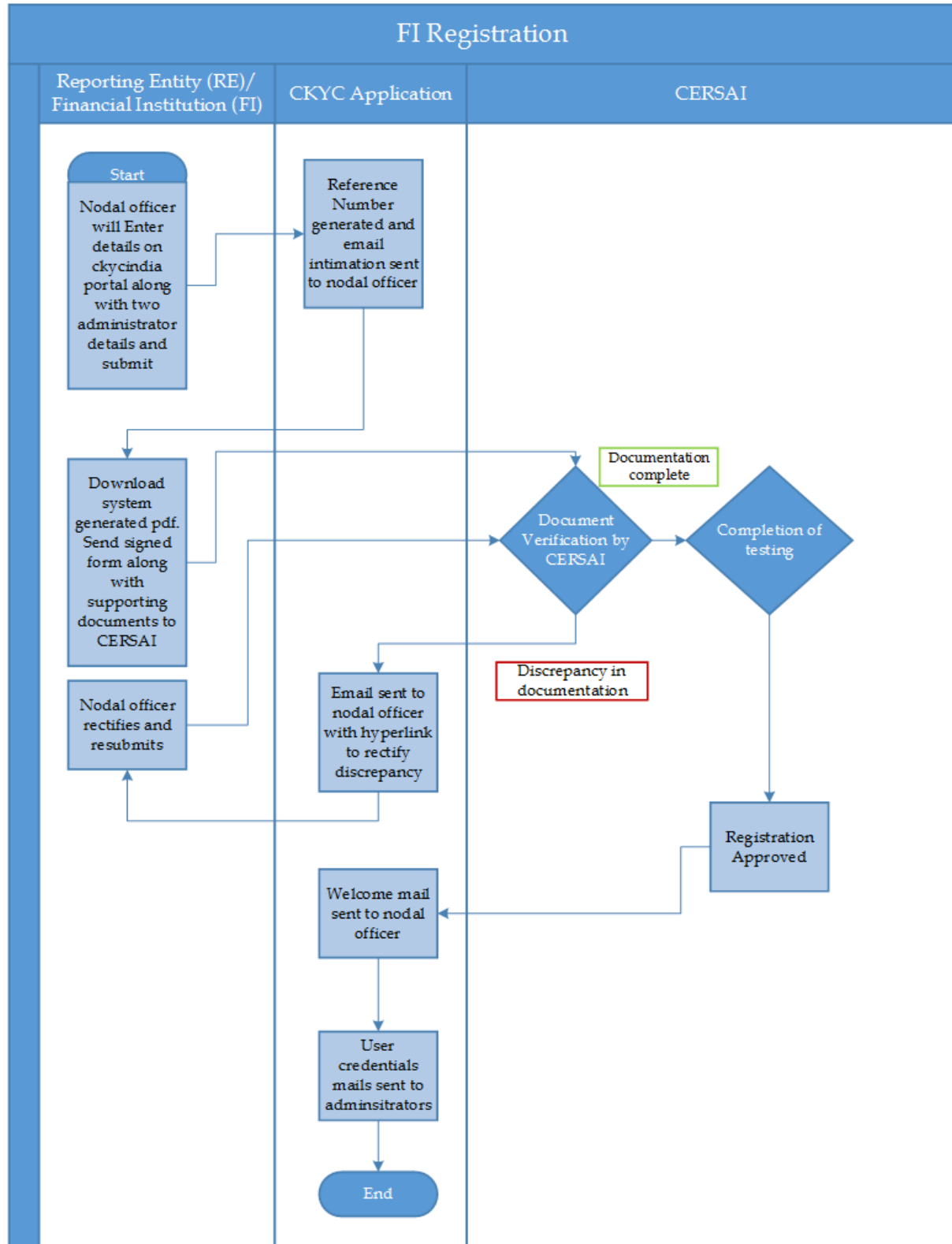
After verification of the documents, Central KYC Registry's administrator will authorize the request for registration of entity.

- i. In case of discrepancies, Registry's administrator shall put the request on hold till the discrepancies are rectified.
- ii. Upon successful registration, user credentials will be emailed to the Admin and Co-Admin users.

User ID and a link for generation of password will be provided to the users on their registered email. For password generation, the reporting entity admin user will be required to click on the link provided in e-mail. The link will redirect the user to the screen for password generation / reset where the user has to enter the registered mobile number. Upon authentication of the mobile

number, an OTP will be sent to the user via SMS which needs to be entered on the screen and then the user may reset the password.

The process flow for Financial institution registration has been illustrated below:



Access hierarchy:

The Admin / Co-admin users of the institutions may create Maker/Checker users as per their institution's requirement. There are three levels of users:

- Institution
 - Admin
 - User
- Region
 - Admin
 - User
- Branch
 - Admin
 - User

All activities e.g. creation/deactivation of users, creation/updation of KYC records, fee payments etc. require Maker-Checker process.

Digital Signature:

- a) Every reporting entity can have access to the CKYCR portal through digital signature.
- b) Digital signature is validated each time.
- c) Type of Digital Signature required is Class II or Class III

SFTP Access:

SFTP access is provided to Reporting entities to upload/download files over a secure connection.

B. Upload of KYC Record

- a) The data captured as per the common KYC template is to be uploaded on the Central KYC portal along with the scanned copy of the supporting documents (PoI/PoA). For an individual record, the signature and photograph is to be cropped separately and uploaded.

- b) The specifications for scanning the supporting documents and photograph are stated below:
 - i. Document should be scanned in grey-scale with a scanning resolution of 150-200 DPI.
 - a. Photograph must be a recent passport size, preferably in colour. However, scanning has to be in colour mode.
 - b. Dimensions 200 x 230 pixels
 - c. Size of photograph should be between 20kb-50kb
 - ii. Acceptable file format : '.tif', '.tiff', '.pdf', '.jpeg', '.jpg'
 - iii. File Size (Maximum Limit): 350 kb for individual KYC record.
- c) The reporting entity can bulk upload the KYC details and scanned images. Images for each record will be required to be zipped separately. The master zip file will be digitally signed by the reporting entity.
- d) Bulk files can be uploaded either at the branch, region or institution level.
- e) The entity should ensure adequate internet bandwidth for bulk upload. Bulk upload is provided via SFTP. For bulk upload of size less than 20 MB the Central KYC front-end application may also be used. Based on validations, a response file will be generated. This file will contain the success records, error records and download records. The response file is available for download from the Central KYC application.

C. Search and Download of KYC record

- a) Reporting entity can search for the record by entering CKYC identifier or by entering a valid ID type and number.
- b) Reporting entity can download single / bulk records by entering CKYC identifier and an authentication factor (viz. date of birth / date of incorporation).

D. Update of KYC record

In case of change of existing information of a customer (including minor turning major) in the records of Central KYC Registry, a reporting entity will initiate an update request.

- a) The updated data along with the scanned copy of the supporting document, where required, will be uploaded on the Central KYC Registry portal.
- b) In order to initiate an updation request, the reporting entity will need to have the latest KYC record of the customer.
- c) On updation of a KYC record at the Central KYC Registry, all linked entities (institutions that have either uploaded or downloaded the KYC record for that particular KYC record), will receive an electronic update notification of KYC record. The entities can download the last updated record of the customer.

E. Multiple correspondence addresses:

Central KYC Registry will enable linkage of multiple correspondence addresses.

An individual can fill Annexure-A1 for multiple addresses and submit the details to the reporting entity which in turn will initiate the update request on the Central KYC application.

F. Processing of Records at Central KYC Registry

De-duplication: The KYC data uploaded on the Central KYC Registry will go through de-duplication process on the basis of the demographics (i.e. customer name, maiden name, gender, date of birth, mother's name, father/spouse name, addresses, mobile number, email id etc.) and identity details submitted. The de-dupe process uses normaliser algorithm and custom Indian language phonetics.

- i. Where an exact match exists for the KYC data uploaded, the reporting entity will be provided with the KYC identifier for downloading the KYC record.
- ii. Where a probable match exists for the KYC data uploaded, the record will be flagged for reconciliation by the reporting entity.

Reconciliation of Probable match:

- a) Central KYC Registry will provide the probable match cases to the reporting entities for reconciliation and resolution.
- b) Where the reporting entity confirms the KYC record as an exact match, it will need to download the existing KYC record of the customer.
- c) Where the reporting entity confirms the KYC record as a 'no match', it shall be forwarded for processing and a unique KYC identifier will be generated for the record.
- d) The reporting entity will have to resolve the probable matches within 5 working days, beyond which the record will be withdrawn by the Central KYC Registry. However, the same can be uploaded as a new record, if 'no match' is found.

ID Match:

The identity detail will be matched by the Central KYC Registry with the ID issuing authority wherever feasible and mechanism is established. Where the ID is not confirmed by the ID issuing authority or the name does not match with the records therein, the record will not be accepted by the Registry and sent back to the reporting entity for verification and uploading again with the updated details.

We may further advise that the ID match wherever feasible with source authority or the de-duplication process by CKYCR Registry does not substitute the statutory/ regulatory obligations to be fulfilled by reporting entities under the respective statutory provisions/regulatory guidelines.

G. KYC Identifier

- a) A 14 digit unique KYC identifier will be generated for new customer records and notified to the reporting entity.
- b) For “Small Accounts” the KYC identifier will additionally have a prefix “S”.
- c) For “Simplified Measures Accounts” the KYC identifier will additionally have a prefix “L”.

H. Fees

- a) Reporting entities can avail services of Central KYC registry on payment of prescribed fee, in advance.
- b) For every service availed, the requisite amount will be deducted from the advance payment made. If the available balance is insufficient, the reporting entity will not be able to avail the services until the balance is replenished.
- c) To make the advance payment, the reporting entity will be required to generate the proforma invoice through the Central KYC application. The reporting entity is required to make an advance payment through NEFT/RTGS in CERSAI's bank account and mention the system generated proforma invoice reference number as the remark.
- d) Upon confirmation of the payment receipt from the bank, balance will be updated. In case of the tax deducted at source (TDS), the reporting entity is required to submit a copy of the TDS certificate to the Central KYC Registry.

- e) Reporting entity will be intimated when the balance goes below the prescribed limit set by them. The reporting entity user can download / print the usage details till the previous day.

V. Reports

- a) Central KYC application shall provide reports including dashboards, access trail and audit trail.

Administration	Operational	Accounts
<ul style="list-style-type: none"> • Log Report • Access Trail • User Master • Institution Master 	<ul style="list-style-type: none"> • Dashboard • Daily MIS • Bulk Upload • Unsolicited Updates 	<ul style="list-style-type: none"> • Ledger

1. Log Report

Log report provides the details of the users of the reporting entity who have logged into the Central KYC application, for a specified period of time.

2. Access Trail

Access trail report provides an admin user, the pages accessed by the users created under his hierarchy on the Central KYC application.

3. User Master

User Master provides the details of the users under the reporting entity for the purposes of accessing Central KYC application.

4. Bulk Upload

Using this report, admin user can view the current status along with the count of records for each uploaded batch.

5. Dashboard

Institution Admin User can view the summary of all uploaded KYC records for a specified time period.

6. Daily MIS

Daily MIS provides the Admin User the details of the uploads for a specified time period.

7. Update Notification

This report provides the notifications for the updates done on a KYC record that is linked to the reporting entity, for a specified time period.

8. Ledger

This provides the summary of the payments made and utilised for the transactions on the Central KYC Registry.

VI. Retention of Records

- a) Central KYC Registry shall ensure retention of the Know Your Customer (KYC) records in an electronic format for a period specified by the rules and shall ensure that the retrieval of the information is facilitated within stipulated time period.

VII. Grievance Mechanism

Central KYC Registry shall provide for the grievances of reporting entities to be redressed in a timely and appropriate manner and ensure records are maintained for such resolution.

Contact details of the Central KYC Registry Helpdesk:

Phone: 022-61102592 (10 lines)

Email: helpdesk@ckycindia.in
