CDSL VENTURES LIMITED

….Exploring New Horizons

PROCESS NOTE

OCTOBER 03, 2022

KRA PROCESS NOTE AS PER SEBI GUIDELINES

We refer to Communiqué number **'CVL/OPS/INTERM/GENRL/22-146'** related to SEBI Circular no. **SEBI/HO/MIRSD/DoP/P/CIR/2022/46** dated April 6, 2022, and subsequent FAQs released by SEBI regarding **'Guidelines in pursuance of amendment to SEBI KYC Registration Agency (KRA) Regulations, 2011'**. The Intermediaries are advised to note the following in accordance:

1. **Additional Option for Gender field introduced:**

    1. 'Transgender' (T) shall be added as a gender option to existing 'Male' (M) and Female (F) options.

2. **KYC fields that would be validated by KRA before verifying the KYC**

    1. Investor's Registered Email ID
    2. Investor's Registered Mobile Number
    3. Investor's PAN details
    4. Investor's Aadhaar Details where Aadhaar is provided as OVD

    If the validation fails, the KYC will be put on Hold with reason as KYC Invalid for respective reason. Investor will be allowed to carry out any transactions (buy/sell) only if KYC is Verified and Validated.

3. **Single digitally signed/e-signed PDF file with KYC Documents**

    In the case of digital KYC modes (mode 1-5), PDF of KYC documents should be digitally signed by the investor. For any modification of existing KYC records, supporting documents with a verifiable e-sign is mandatory. Intermediaries are required to provide KYC document images in a single PDF file.

1. The PDF file should be digitally signed or e-signed by the Investor.
2. The validity of the e-sign would be ascertained in case of modification KYC. KYC documents with invalid digital signature/e-sign would not be accepted.
3. The applicant's name and the e-sign name would be matched with threshold of 90%.
4. The Order of KYC Documents in PDF file should be:
   i. KYC application form
   ii. POI → PAN / e-PAN
   iii. POA → E-Aadhaar / Extracted Aadhaar data from Aadhaar XML
   iv. Applicant Wet Signature Page
5. Digital Signature validity flag would be maintained by KRA for KYC. Digital Signature validation flag may be changed by operator IF AND ONLY IF it is failing due to name match threshold.
6. The naming convention of PDF file should be **<PANNUMBER>.PDF**
7. This is applicable for all digital KYC modes (1 - 5)

4. Process for Email & Mobile Validation:

1. Default Process

1) Intermediary to intimate investor that email and mobile verification link shall be shared by CVL KRA, and to click on the verification links provided in both email and mobile SMS for validating the KRA registered email ID and mobile number.
2) CVL KRA triggers email and SMS with verification link to the registered email ID and mobile for concerned PAN.
3) CVL relies on confirmation action (click on verification link) by investor to validate the investor's email address and mobile number.
4) If confirmation action is not taken by investor, the email ID and mobile validation would be based on delivery report.
5) The verification SMS and email would be re-triggered to investors, maximum 3 times every 6 hours, until the mobile number and/or email ID is validated.
6) Email and Mobile validation are not mandatory for KYCs processed with Non-Aadhaar OVD.

2. **API Process for email/mobile validation process:**
   This is an optional service provided by CVL which the intermediaries may avail.

   1) Investor visits SRI (SEBI Registered Intermediary) portal for KYC registration (new/mod)
   2) Investor Enters PAN number, Email address, and Mobile Number
   3) A Push API is triggered by SRI to KRA, sharing following information:
      a. PAN
      b. Email address
      c. Mobile number
      d. License No.
      e. Flag to determine what to validate (0 – email, 1 – mobile, 2 – both)
      f. SRI Unique code given by KRA or Intermediary Code
      g. Unique serial no. for each request.
      h. Request Date and Time
   4) KRA receives API request and generates and sends OTP to the investor email and mobile. (Delivery report is tracked and delivery flag updated accordingly)
   5) KRA will confirm back to SRI
      a. PAN
      b. Unique serial no. sent by SRI.
      c. KRA unique reference no.
      d. Flag to determine what to validate (0 – email, 1 – mobile, 2 – both)
      e. Status flag (Success/Fail)
   6) Post confirmation from KRA, SRI will ask Investor to enter the OTP received email and/or mobile OTP on SRI portal.
   7) SRI will collect and call validate API to KRA for confirmation
      a. PAN
      b. SMS OTP
      c. Email OTP
      d. SRI Unique serial No, which sent by SRI in first request
      e. KRA unique reference no. sent by KRA in response to SRI request
      f. Flag to determine what to validate (0 – email, 1 – mobile, 2 – both)
   8) KRA will validate the OTP and confirm back to SRI
      a. PAN
      b. SRI Unique serial No, which sent by SRI in first request
      c. KRA unique reference no. sent by KRA in response to SRI request
      d. Flag to determine what to validate (0 – email, 1 – mobile, 2 – both)

e. SMS OTP Confirmation Y – OTP matched / N – OTP mismatched / X – OTP matching not requested
f. EMAIL OTP Confirmation Y – OTP matched / N – OTP mismatched / X – OTP matching not requested

5. Process for Aadhaar Validation:

Specific consent needs to be taken from investors for sharing the AADHAAR data and documents with KRA for validation purposes. This **consent also needs to be declared on KYC Application Form.** The shared documents and data will be used by KRA to validate the KYC information uploaded by SRI. The content of the consent shall be shared by KRA separately.

The process and requirements based on KYC Modes is as follows:

1. Physical KYC (KYC Mode 0)

Following points are to be noted while processing Physical KYC (mode 0) where Aadhaar copy uploaded by investor is used as proof of address.

i. **Scanned Aadhaar/E-Aadhaar with masked Aadhaar number** of the investor needs to be uploaded for KYC verification.
ii. **If unmasked Aadhaar number appears** anywhere on the KYC document, including Aadhaar copy, KYC Application form, or on PAN copy, the **KYC would be rejected.**
iii. Aadhaar data **validation would be performed based on the Aadhaar QR** code. Aadhaar copy without the QR code would not be accepted, and KYC would remain in INVALID status.
iv. Intermediary to ensure that scanned Aadhaar/E-Aadhaar with readable QR code (resolution 200 dpi +) is provided by investor. **It is highly recommended that E-Aadhaar with masked Aadhaar number be provided** instead of scanned Aadhaar copy. E-Aadhaar can be downloaded by the investor from UIDAI site.
v. Intermediary to **upload the clear Scanned Aadhaar /E-Aadhaar copy as part of supporting documents** (over SFTP/frontend). The naming convention of the entire set of documents should be **<PANNUMBER>.PDF**. If Aadhaar Scan copy/ E-Aadhaar is being uploaded as a separate file, the naming convention should be **<PANNUMBER>_AADHAAR.PDF**

vi. QR codes on Aadhaar copy submitted that could not be scanned would result in INVALID KYC status and will be put on HOLD.

vii. Aadhaar number should be masked in such a way that **first 8 digits of Aadhaar is masked, and last 4 digits are readable**. If the Aadhar number is not masked as required, the KYC would be rejected.

2. Online eKYC – OTP (KYC Mode 1)

i. SRI uploads the XML file received from UIDAI on the frontend/SFTP server in the location provided by KRA

ii. The **XML issuance date should not be older than 3 days** from the date of KYC submission by the Investor.

iii. The UDIAI digital signature hash in the XML file would be validated by KRA.

iv. The **naming convention for Aadhaar XML file** being uploaded should be **<PANNUMBER>.XML**

v. CVL picks the XML file from SFTP server, processes the file to further validate the address in KYC meta-data and KYC application (OCR) provided by the SRI against the Aadhaar XML file.

Validation parameters and Threshold:

Sr No.	Parameter to Validate	Threshold for Validation
1.	NAME	90%
2.	GENDER	100%
3.	PHOTO	50%
4.	ADDRESS Pin-code State Country	80% 100% 100% 100%

3. Online KYC (KYC Mode 3)

Following points are to be noted while processing Online KYC (mode 3) where Aadhaar copy uploaded by investor is used as proof of address.

i. **E-Aadhaar with masked Aadhaar number** of the investor needs to be uploaded for KYC verification.

ii. **If unmasked Aadhaar number appears** anywhere on the KYC document, including Aadhaar copy, KYC Application form, or on PAN copy, the **KYC would be rejected.**

iii. Aadhaar data **validation would be performed based on the Aadhaar QR** code. Aadhaar copy without the QR code would not be accepted, and KYC would remain in INVALID status.

iv. Intermediary to ensure that E-Aadhaar with readable QR code (resolution 200 dpi +) is provided by investor by redirecting the investor to UIDAI site to download the E-Aadhaar with masked Aadhaar number and upload the Aadhaar copy.

v. Intermediary to **upload the E-Aadhaar copy as part of supporting documents** (over SFTP/frontend). If E-Aadhaar is being uploaded as a separate file, the naming convention should be **<PANNUMBER>_AADHAAR.PDF**

vi. Aadhaar XML/Digilocker XML file uploaded instead of masked E-Aadhaar would not be accepted for this KYC mode and would be subject to rejection.

vii. QR codes on Aadhaar copy submitted that could not be scanned would result in INVALID KYC status and will be put on HOLD.

viii. Aadhaar number should be masked in such a way that **first 8 digits of Aadhaar is masked, and last 4 digits are readable**. If the Aadhar number is not masked as required, the KYC would be rejected.

4. Offline eKYC (KYC Mode 4)

i. Investor is redirected by SRI from its portal to UIDAI website for downloading the Offline Aadhaar ZIP file.

ii. Investor uploads the Offline Aadhaar ZIP file on SRI Portal and enters the passcode.

iii. SRI unzips the file and renames the source XML file as <PANNUMBER>.XML

iv. SRI uploads this file on the frontend/SFTP server in the location provided by KRA

v. The **XML issuance date should not be older than 3 days** from the date of KYC submission by the Investor.

vi. The UIDAI digital signature hash in the XML file would be validated by KRA.

vii. CVL KRA picks the <PANNUMBER>.XML file from SFTP server along with digitally signed/e-signed KYC Documents PDF file and processes the same to further validate the details in KYC meta-data and KYC application form provided by the SRI against Aadhaar source XML file.

Validation parameters and Threshold:

Sr No.	Parameter to Validate	Threshold for Validation
1.	NAME	90%
2.	GENDER	100%
3.	PHOTO	50%
4.	ADDRESS Pin-code State Country	80% 100% 100% 100%

5. **Digilocker KYC (Mode 5)**

   i. Investor is redirected by SRI from its portal to provide consent to SRI to get Digilocker signed XML response file.
   ii. SRI receives the Digilocker signed XML response file
   iii. SRI uploads this file on the frontend/SFTP server in the location provided by KRA
   iv. The **XML issuance date should not be older than 3 days** from the date of KYC submission by the Investor.
   v. The UDIAI digital signature hash in the XML file would be validated by KRA.
   vi. The **naming convention for Digilocker XML file** being uploaded should be **<PANNUMBER>.XML**
   vii. CVL picks the Digilocker XML file from SFTP server, processes the file to further validate the address in KYC meta-data and KYC application (OCR) provided by the SRI against Digilocker Aadhaar XML file.

   Validation parameters and Threshold:

Sr No.	Parameter to Validate	Threshold for Validation
1.	NAME	90%
2.	GENDER	100%
3.	PHOTO	50%
4.	ADDRESS Pin-code State Country	80% 100% 100% 100%

6. **PAN Status validation –**

   i. PAN validation will be carried out by KRA at the moment the KYC application is processed/submitted by SRI to KRA

ii. KRA accepts the KYC request (new/mod) and checks PAN status with ITD
iii. Based on response from ITD, PAN flag and Status is updated in KYC.
iv. Details checked from ITD response
    1) PAN Status
    2) IT Site PAN Name
    3) Aadhaar Seeding
v. Based on response from ITD, KRA either:
    1) Partially processes request and marks KYC status as Under Process, until documents are received, OR
    2) Rejects KYC with PAN status as reason (Invalid/Fraud)

7. **The TAT for processing KYC from the date of receiving all KYC documents & required data from intermediary would be T+2 Days**, where Aadhaar as OVD is provided.

8. **KYC documents need to be uploaded only at one place** - either on SFTP (preferred) or on front end, and not at both places to avoid delay in KYC processing due to process lock and failure.

9. Intermediary to select appropriate KYC mode while raising New/Fresh or Modification KYC. **Incorrect KYC mode selection would result in auto-rejection** of concerned KYC request. KYC mode details are as follows:

Mode	Name	Description
Mode 0	Physical KYC	In this mode the KYC documents are processed physically. Physical In-Person-Verification (IPV) is required. The applicant physically signs the KYC documents. Document Requirement: Physically signed KYC documents with IPV. Scanned and masked Aadhaar with readable QR code.
Mode 1	EKYC OTP	The KYC documents are processed online and authenticated using Aadhaar/EKYC OTP by Sub-AUA/Sub-KUA. IPV is not required. Document Requirement: Applicable only for Sub-AUA/Sub-KUA

Mode 2	EKYC BIOmetric	The KYC documents are processed online and authenticated using Aadhaar/EKYC Biometric records in UIDAI database by Sub-AUA/Sub-KUA. IPV is not required. Document Requirement: Applicable only for Sub-AUA/Sub-KUA
Mode 3	Online KYC	The KYC documents are processed online where Virtual In-Person-Verification (VIPV) is carried out. The documents are e-signed by the applicant. The Source of Aadhaar (or any Address Proof) is the Applicant. Eg. Scanned copy provided. Document Requirement: e-Signed KYC documents with IPV, masked E-Aadhaar with readable QR code.
Mode 4	EKYC Offline	The KYC documents are processed online and e-signed by applicant. The source of Aadhaar XML as Address proof is UIDAI offline eKYC. IPV is not required. Document Requirement: e-Signed KYC documents, Offline Aadhaar XML file.
Mode 5	Digilocker KYC	The KYC documents are processed online and e-signed by applicant. The source of Aadhaar XML as Address proof is Digilocker. IPV is not required. Document Requirement: e-Signed KYC documents, Digilocker XML file.

10. For modifications only in following fields of KYC details, only **e-signed KYC Application Form** for digital modes and **physically signed KYC Application Form** for physical mode would be **mandatorily required.** Other supporting documents (POI/POA) are not required. The KYC should be raised with document flag as 'Without supporting Documents'.

Type of KYC details	Individual Category of investor	Non-Individual Category of investor
Identity Details	Father's/Spouse	
	Marital Status	
Address Details	Telephone Number	Telephone Number
	Mobile Number	Mobile Number

	Email ID	Email ID
	Fax	Fax
Other Details	Gross Annual Income Details/Net Worth	
	Occupation	
	PEP Status	
	Any other Information	Any other Information

If Email ID and/or Mobile number is modified without supporting document, the changed email ID and mobile number shall be validated, irrespective of Aadhaar/Non-Aadhaar OVD based KYC.

11. For Inter-Operability 'KYC Inquiry' (IOP1) (for both Original and Modified), KRAs would share **additional tag/field called 'Proof of Address type'**, to indicate whether the KYC is Aadhaar OVD based or Non-Aadhaar OVD based KYC. Value 31 returned under this new tag shall indicate that KYC is AADHAAR OVD based.

12. A new KYC status code "07" (KYC VALIDATED) shall be added to the existing status codes of KYC. The status for verified and valid KYC for KYCs raised post 1st November 2022 would be '07'. The list of status codes for a KYC record with their description are provided below which will be common across all KRAs.

Code	Description
01	UNDER_PROCESS
02	KYC REGISTERED
03	ON HOLD
04	KYC REJECTED
05	NOT AVAILABLE
06	DEACTIVATE
07	KYC VALIDATED
11	OLD RECORD UNDER PROCESS
12	OLD RECORD KYC REGISTERED

13	OLD RECORD ON HOLD
14	OLD RECORD KYC REJECTED
22	MUTUAL FUND VERIFIED

13. For **Existing KYC** and **KYCs raised up to 31st October 2022** the status for Verified KYC would be continue being in status '02' and shall continue to exist in the system. Post validation of the existing records where AADHAAR is OVD, KYC status would change to '07' - KYC Validated. The validation would commence from the go live date of November 01, 2022 and would be completed within 180 days of go live.

14. **The tags/file structure** with values passed in the same **for download/response to intermediaries from KRAs would continue to be the same** as what is prevalent as on date.

15. The file structure for upload would have an additional tag/field for passing **'District'** value.

16. For existing KYCs and KYCs (new/modification) raised with **OVD as Non-Aadhaar, there is no change in the existing process of KYC verification.**

17. The process and TAT for KYC raised with **Non-Aadhaar OVD remains unchanged.**

18. The **effective date** for implementation for the process outlined here is **1st November 2022.**

A table is enclosed for validation to be done by KRAs based on the type of OVDs marked below (refer – Annexure)

ANNEXURE

OVD	Validation of Email Address by KRAs	Validation of Mobile Number by KRAs	Validation of PAN by KRAs	Validation by KRAs of Aadhaar which includes validation of Name, Gender, address, photo)	Timelines for processing by KRAs post upload of KYC data and documents by SRI	Impact
Aadhaar XML file (Digilocker KYC, AADHAAR Offline Zip file KYC)	Yes	Yes	Yes	Yes	T+2 days (T is date of receipt of KYC data and documents from SRI)	As per SEBI directions, SRI shall allow transactions only after the independent validation of KYC records is done by concerned KRA
Aadhaar card/ PVC card/ eAADHAAR image with QR code (Normal KYC/ Online KYC)	Yes	Yes	Yes	Yes	T+2 days (T is date of receipt of KYC data and documents from SRI)	As per SEBI directions, SRI shall allow transactions only after the independent validation of KYC records is done by concerned KRA
Non-Aadhaar as OVD	Will continue to be verified as per extant process by KRAs	Will continue to be verified as per extant process by KRAs	Will continue to be verified as per extant process by KRAs	Not applicable (non-Aadhaar document as OVD)	No change in TAT	Not applicable