

Government of India
Ministry of Communications
Department of Telecommunications
Access Services Cell
Sanchar Bhawan, 20, Ashoka Road, New Delhi - 110 001

File No: 800-12/2021-AS.II

Dated: 31.08.2021

To,

All Unified Licensees (having Access Service Authorization)/ Unified Licensees (AS)/ Unified Access Services Licensees/ Cellular Mobile Telephone Service Licensees

Subject: Proof of Concept (PoC) of Self-KYC (S-KYC) as an alternate process for issuing of new mobile connections to Individual and Outstation category customers.

Online service delivery has become an acceptable norm in all sectors in recent past and most of the citizen centric services are being offered through internet. Contactless services in the present era are to be promoted for subscriber convenience and also for ease of doing business. Presently, a subscriber has to undergo Know Your Customer process which entails visit to the Point of Sale along with the original documents of identity and address as proof for obtaining new mobile connection.

In this regard, an alternate online Self-KYC (S-KYC) process is being proposed. Licensees who are willing to offer this alternate S-KYC process to their customers are hereby directed to ensure readiness of their systems and offer the PoC of the process for approval. The procedure to be followed for issuing mobile connections using the S-KYC process broadly includes the registration of the customer, CAF filling process for respective customer category, electronic verification of the PoI/PoA of the customer, delivery of SIM card, verification by the Licensee and SIM activation.

2. Registration of the customer

- i.) The customer shall download the authenticated application (App) of the Licensee from the app store on his/her mobile.
- ii.) The customer shall register himself/herself on the App using his/her mobile number. The mobile number shall be customer's own alternate mobile number. The registration process shall include the successful verification of time based

Yash Kumar

One Time Password (OTP) sent on the mobile number provided by the customer. However, if the customer does not have any own alternate mobile number, then mobile number of his/her family members/relatives/known persons may be used for this purpose and be clearly mentioned in Customer Acquisition Form (CAF).

- iii.) The Licensee shall ensure that the alternate number provided by the customer for registration in the App shall be the mobile number of India.
- iv.) Login-ID shall be the mobile number used for registration by the customer. For logging in the app, customer will be provided with an unique time-based OTP (TOTP). Further an unique TOTP is re-generated & sent to customer's registered mobile number for every/ new login attempt.
- v.) The unique CAF shall be created by the Licensee in the app after successful validation of the OTP sent on the mobile number used for the registration.
- vi.) If the alternate number provided by the customer is of his/her family members/relatives/known persons, then after successful verification and activation of the new mobile connection, the mobile number provided and linked with the login-ID shall be replaced with the mobile number allotted to the customer.
- vii.) The above mentioned registration can also be done on the authorized website/portal of the Licensee using desktop/laptop.

3. Verification of valid documents for the S-KYC process

- i.) Only those PoI/PoA documents shall be applicable for this process which can be electronically verified by the Licensee from the issuing authority of such documents.
- ii.) The electronically verified PoI/PoA documents may be obtained by the Licensee from the DigiLocker. Only those documents, which have been issued and verified by the issuing authority on DigiLocker, shall be used for the purpose of subscriber verification. In no case, the documents uploaded by the customers on the DigiLocker shall be used for the subscriber verification process.
- iii.) In case Aadhaar card is used by the customer, the electronic verification may be done by the OTP based Authentication of UIDAI.

In this process, an OTP with limited time validity (TOTP), is sent to the mobile number and/ or e-mail address of the customer registered with the UIDAI. The customer shall provide this OTP along with his Aadhaar number during authentication and the same shall be matched with the OTP generated by the UIDAI. In this, complete e-KYC details along with

photograph of the customer is received by the Licensee from the UIDAI.
The received file shall be in the xml format.

If Aadhaar card is used in this process, following declaration/consent shall be taken from the subscriber:

- *I am voluntarily using Aadhaar based authentication for acquiring the SIM.*
- *I hereby give my consent to use my Aadhaar number/Virtual-ID verified by OTP received on my Aadhaar linked mobile number by UIDAI for sharing the KYC details (demographic data and photograph) from my Aadhaar to the TSP name for issuing of mobile connection to me.*

iv.) All records pertaining to the verification of PoI/PoA documents as received from the issuing authority of such documents shall be stored by the Licensee.

4. Customer Acquisition Form (CAF) filling process

- i.) Before initiation of the CAF filling process, the customer shall be asked to declare that he/she is in possession of the original PoI/PoA documents and in case any forgery is found in his/her documents at any later time, necessary action as per law of the land shall be applicable on him/her.
- ii.) The customer shall be asked to choose the electronic verification he/she wishes to undertake (out of Aadhaar or DigiLocker).
- iii.) In case of Aadhaar, OTP based authentication as mentioned in Para 3 is conducted for electronic verification and obtaining demographic details from the UIDAI. In case of DigiLocker, the PoI/PoA documents as selected by the subscriber shall be transferred to the Licensee as mentioned in Para 3.
- iv.) In case of Aadhaar, all the fields as received from UIDAI shall be automatically captured in the CAF by the Licensee. All other mandatory & required fields in the CAF shall be manually filled by the customer.
- v.) For all other documents, customer shall be asked to access his/her DigiLocker account and transfer the electronically verified PoI/PoA documents to the Licensee. The Licensee shall store the PoI/PoA documents as received from the DigiLocker.
- vi.) In case of DigiLocker, all the entries in the CAF shall be filled using fields available in XML received from DigiLocker. All other mandatory fields in CAF shall be manually filled by the customer as per the original PoI/PoA.
- vii.) After this, the customer shall be asked to capture the live photograph of himself/herself. The customer shall also be asked to record his/her live video and read out his /her name and Date of Birth (DoB) in the video which shall be of minimum 10 seconds. The customer shall also be asked to display certain

gestures including blinking of eyes while recording of the video. The customer shall also be asked to read out randomly generated alphanumeric minimum 06-digit CAPTCHA during recording of the live video.. In case this 10 second video is required to be saved at TSP's end for audit purposes, then after 90 days the video will be archived in offline mode and if required, TSPs will be able to retrieve & furnish the video only by 72 hours of receiving such a request.

- viii.) The Licensee shall ensure that the live photograph of the customer is embedded in the CAF. Further, the system application of the Licensee shall put a watermark in readable form having CAF number, GPS coordinates, and Date (DD:MM:YYYY) & time stamp (HH:MM:SS) on the captured live photograph of the customer.
- ix.) The App/website/portal of the licensee shall have the feature that only live photograph of the customer is captured and no printed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white color or any other light & plain background and no other person shall come into the frame while capturing the live photograph of the customer.
- x.) The live photograph and live video of the customer shall be captured in proper light so that they are clearly visible, audible and identifiable.
- xi.) The capturing of the live photograph and recording of live video shall be done by the App/website/portal and in no case customer shall be allowed to upload any file, document, video etc. using the App/website/portal.
- xii.) Before dispatch of SIM card to the customer, if any discrepancies are found by the Licensee in the CAF, the same may be intimated to the customer and customer may be asked to make the desired modifications in the CAF which are in conformity to this process including existing instructions for subscriber verifications. All such communications including pre-modified entries, pictures etc. of the customer shall be kept on record by the Licensee. In no case, modifications shall be made in the CAF after dispatch of the SIM card.

5. Local Category customer

- i.) If the local and permanent addresses provided by the customer are of same LSA, the customer may be treated as Local Category.
- ii.) The procedure mentioned at Para 4 shall be followed.
- iii.) After this, the customer shall be required to provide the following declaration: -

- a) *All the details provided by me are correct and the documents attached by me are authentic and if found forged, actions as per the law of the land shall be applicable to me.*
- b) *I am an ordinary resident of India and am using the App/website/portal for acquisition of SIM within territorial boundaries of India.*

[For this declaration, an OTP message containing the texts that “please verify the details filled in form before sharing the OTP” shall be sent to the mobile connection of the customer used for the registration. Upon successful OTP validation, it shall be treated as signature of the customer on the declaration.]

6. Outstation Category customer

- i.) If the local and permanent addresses provided by the customer are of different Licensed Service Areas (LSAs), the customer shall be treated as Outstation Category customer.
- ii.) In addition to the procedure mentioned at Para 4, the customer shall be asked to provide his/her local address in the LSA and details of a local reference in the LSA.
- iii.) The verification of local reference may be done by sending an OTP on the mobile number of local reference submitted by customer and upon successful OTP validation only, the local reference may be treated as tele-verified.
- iv.) The Licensee shall ensure that the mobile number used for the local reference shall not be used for activation of more than nine mobile connections.
- v.) The mobile number used for registration and for local reference shall not be same.
- iv.) After this, the customer shall be required to provide the following declaration: -
 - a) *All the details provided by me are correct and the documents attached by me are authentic and if found forged, actions as per the law of the land shall be applicable to me.*
 - b) *I am an ordinary resident of India and am using the App/website/portal for acquisition of SIM within territorial boundaries of India.*[For this declaration, an OTP message containing the texts that “please verify the details filled in form before sharing the OTP” shall be sent to the mobile connection of the customer used for the registration. Upon successful OTP validation, it shall be treated as signature of the customer on the declaration.]

7. Verification by the Licensee before delivery of SIM card.

- i.) Before delivery of SIM card, the authorized representative or the IT system of the Licensee shall check and verify, not limited to, the following:
 - a) All the entries in the CAF & Licensee's database including the mandatory fields for the respective customer are complete and there is no error apparent on the face of records of the customer in the CAF & database.
 - b) Live photograph of the customer is ample clear and customer can be identified using the photograph.
 - c) No gibberish information is stored in the CAF and Licensee's database.
 - d) Completeness and correctness of all necessary documents attached by the customer.
 - e) The Latitude/Longitude captured in the CAF are well within the territorial boundaries of the country.
 - f) The photograph as available on the PoI matches with the live photograph of the customer as captured on the CAF. (In case of DigiLocker only)
 - g) The photograph as received from the Aadhaar matches with the live photograph of the customer as captured on the CAF. (In case of OTP based authentication of UIDAI)
 - h) The CAPTCHA read out by the customer during the recording of live video is same as shown to the customer during filling of CAF.
- ii.) After the successful abovementioned verification, the digital signature on the CAF shall be put by the Licensee.
- iii.) Only after this activity, the SIM shall be dispatched for the delivery to the local address mentioned by the customer.
- iv.) The CAF shall not be modified after fixing of signature by the Licensee.

8. Delivery of SIM Cards (inactive SIM)

- i.) The inactive SIM card shall be delivered at the local address provided by the customer in the CAF.
- ii.) During the delivery of SIM card to the customer at the local address mentioned in the CAF, the Latitude/Longitude shall be captured by the authorized representative of Licensee. SIM card should be delivered to customer or to the customer's representative available at the local address after confirming and validating OTP sent on customer's registered number.
- iii.) As soon as the SIM is delivered to the customer, a configuration SMS shall be sent to the mobile number provided by the customer during the registration process mentioning that the *SIM with mobile number..... has been delivered*

at your address, if not received, please contact(the Licensee's details shall be provided).

- iv.) After receipt of the inactive SIM card, customer will re-login into the app/website/portal. The customer will be asked to enter/scan the 19-digit ICCID number printed on the SIM card. An OTP mentioning that kindly verify the possession of the SIM card shall be sent on customer's mobile number provided. After successful verification, the Licensee shall follow the validation at their backend.
- v.) The SIM shall be delivered to the local address mentioned in the CAF within 7 days of dispatch of SIM by the Licensee. If the SIM could not be delivered at the local address mentioned in the CAF due to incomplete address details or any other reasons whatsoever, the customer shall be intimated via email and text messages that the delivery will be tried one more time and if the customer would not be available at the address, the SIM shall be sent back to the store and customer shall have to again apply for the acquisition of mobile connection. Also, in case the customer is not found at the address at the second time of delivery of SIM card, the Login-ID may be blocked for 7 days and customer would not be able to order SIM using this process for 7 days.

9. e-SIM card

- i.) In case of e-SIM card, the para 8.above shall not be applicable.
- ii.) Licensee shall ensure that the S-KYC App shall only be installed on the mobile in which customer is desirous of obtaining mobile connection.
- iii.) In addition to the procedure mentioned at Para 3. to Para 7. above, the embedded SIM-ID (EID) and IMEI number of the mobile phone shall be automatically captured/manually entered by the Licensee and the same shall be used for generation of virtual-SIM. EID and IMEI shall also be captured in the CAF by the Licensee.

10. Verification by the Licensee before SIM Activation

- i.) Before activation of the mobile connection, the Licensee/authorized representative of the Licensee shall check and verify, not limited to, the following :
 - a) All the verifications done at 7i.) above.
 - b) The SIM has been delivered at the local address mentioned in the CAF.
- ii.) On successful verification, the CAF shall be digitally signed by authorized representative of the Licensee/IT system. Only after this activity, the SIM card shall be activated and tele-verification as per the prevailing guidelines shall be

done before final activation of the services. However, if the customer has given his own alternate mobile number, then tele-verification through the use of 5-digit OTP pin shall be done for activation of final services.

iii.) The authorized representative/IT system of the Licensee who conducts the verification before delivery of SIM card shall not conduct the verification before activation of SIM card. The Licensee shall develop such a system that the two representatives of Licensee who conducts the verification shall in no case be able to see each other's identity during the entire process. Moreover, the line of chain of verification done by the two authorized representatives shall also be dynamic in nature.

11. The access of the App/website/portal shall be controlled by the Licensees and it should be ensured that the same is not used by unauthorized persons. The App/website/portal shall be accessed only through login-id & password-controlled mechanism given by Licensees to its customers.

12. The Licensee shall provide adequate information to the customer via video and text mentioning the CAF filling process in details, Do's & Don'ts and identification of the customer category viz. Local or Outstation category. If any discrepancy is found by the Licensee in the selected customer category, the CAF filling process shall be stopped and customer shall be informed to choose the correct customer category for filling the CAF.

13. Customer shall access application hosted on Licensee's server. Licensee should ensure that the application shall not have capability to access local file system of the customer's device for either read or write with exception to only read access to device drivers and all process data should be accessed from Licensee's Server only.

14. The Licensee shall use appropriate encryption regime to ensure security of data-in-transit pertaining to S-KYC process, besides security of data-at-rest (at Licensee nodes). For ensuring privacy/ data security requirement, Licensee shall use suitable mechanism/ IT infrastructure at the Licensee nodes which need to be regularly vetted by Licensee. The Licensees shall ensure compliance to confidentiality/ privacy/ security of customer information keeping in view the law of land and all the relevant license conditions. Any violation shall attract penalties/actions as per license conditions and law of the land.

15. The login shall have a time out of maximum thirty minutes. Moreover, if no activity is observed on the App/website/portal for a continuous period of fifteen

minutes, the active process on the App/website/portal shall be terminated. Customer shall be required to re-login for re-initiating the process.

16. This process is applicable for Local and Outstation category customer and only two mobile connections per day can be issued to a customer using S-KYC process.

17. The Licensee shall develop such a system using latest technological tools including artificial intelligence (AI) to ensure that the S-KYC option in App/website/portal shall only be used within territorial boundaries of India. The Licensee shall also use advanced tools to ensure the liveness of the entire process.

18. The Licensee shall ensure that the entire process shall be conducted using authenticated applications (App) hosted by the Licensees. The entire process may also be conducted using the authenticated website/portal of the Licensee with the same safety features as entrusted on the App of the Licensee

19. In case of authentication through Aadhaar, customer will online authorize UIDAI through Aadhaar authentication using his/her Aadhaar number/Virtual-ID and OTP to provide his/her demographic data as in their database (name of the customer, address, date of birth, and gender) along with his/her photograph (digitally signed and encrypted format) to the Licensee. The digitally signed e-KYC data (demographic data and photograph) provided by UIDAI shall be stored by Licensee as the subscriber record in their database for purpose of issuing mobile connections.

20. For the purpose of identification of a person (customer) using Aadhaar, the Aadhaar number/Virtual-ID of the person shall not be stored by the Licensees.

21. The demographic details of customer along with photograph received from UIDAI shall automatically get captured/populated by the Licensee in read only and un-editable format on the CAF. Rest of the fields like 'Name of Father/Husband' etc., in CAF shall be entered by customer.

22. For every authentication, UIDAI will give a unique response code with date & time stamp and will send the same to Licensee. All the response codes along with date & time stamp received by Licensee during the process shall be automatically captured in the relevant fields of CAF and shall also be stored in database of Licensee.

23. Similarly, unique response code with date & time stamp received from DigiLocker in respect of transfer of PoI/PoA documents of customer to the Licensee the process shall be automatically captured in the relevant fields of CAF and shall also be stored in database of Licensee.

24. The demographic data received from UIDAI shall be stored directly by the Licensee in database. The digitally signed e-KYC response received from UIDAI must be stored & supplied as it is for audit purposes as per existing guidelines for CAF storage & supply respectively and should not be edited/ altered/changed/modified/overridden by the Licensee under any circumstances. Also, if for the Audit/investigation, the digitally signed e-KYC response received from UIDAI is not supplied to LSA Field unit (erstwhile TERM Cell) within given time frame (missing digitally signed e-KYC response cases), the connection shall be treated as pre-activated.

25. Similarly, the PoI/PoA documents received from the DigiLocker shall be directly attached with the CAF. The digitally signed response received from DigiLocker must be stored & supplied as it is for audit purposes as per existing guidelines for CAF storage & supply respectively and should not be edited/ altered/changed/modified/overridden by the Licensee under any circumstances. Also, if for the Audit/investigation, the digitally signed response received from DigiLocker is not supplied to LSA Field unit (erstwhile TERM Cell) within given time frame (missing digitally signed response cases), the connection shall be treated as pre-activated.

26. The Licensee shall ensure that the application shall not have capability to access local file system of the device at customer for either read or write with exception to only read access to device drivers and all process data should be accessed from Licensee's Server only. The application shall nowhere store any data including biometric information and should be compliant with Aadhaar e-KYC and Authentication service and Application Program Interface (API) specifications.

27. The above mentioned S-KYC process is an alternative process in addition to the existing process of issuance of mobile connections to Local customers and shall be applicable for Outstation customers.


28. In case the hard copy of CAF is required by LEAs, it shall always be provided within the prescribed time frame.

29. As and when any Licensee implements the alternate S-KYC process, the same shall be implemented only after complete testing and verification is done by the department in consultation with the security agencies/UIDAI/DigiLocker. The decision regarding implementation of the process shall be taken after assessment of the outcome of the PoC

30. The SKYC process shall be applicable in the all Licensed Service Areas (LSAs) including J&K, North East and Assam LSAs.

31. Any non-compliance observed in the issuing of SIM card and subsequent activation of mobile connections using this process, the Licensee shall be considered as violating the terms and conditions of the License agreement and necessary actions in terms of the License agreement and instructions related to subscriber verifications shall be initiated against the Licensee.

32. The existing instructions in general and particularly those issued vide letter No. 800-09/2010-VAS dated 09th August 2012 and all other instructions shall remain the same for issuing of mobile connections to the new subscribers.


(Suresh Kumar)
ADG (AS-II)
31.08.2021

Copy to:-

1. DG(T), DoT HQ with a request to depute representative for validation of the POC.
2. CEO, UIDAI with a request to depute officials for validation of the PoC
3. President & CEO, NeGD with a request to depute officials for validation of the PoC.
4. JS(CIS), MHA with a request to depute officials for validation of the PoC
5. COAI, New Delhi

Note:- The PoC is required to be done at places to be decided and directed by the O/o DG-T. The TSPs who are ready with the process shall offer the same to the concerned LSAs.