HOW TO LINK MOBILE NUMBER TO AADHAAR

On TSP's website

- Resident to enter the mobile number (to be verified) on wesbite
- TSP will generate an OTP on the entered mobile number which resident will then enter on the website
- Consent message will be displayed on the website and resident will enter the Aadhaar number after checking the consent box

TSP will generate an OTP request to UIDAI

- If there is any mobile number registered with Aadhaar, resident will receive the OTP on it
- Resident will receive a consent message for receiving e-KYC from UIDAI and resident will enter OTP after providing the consent
- Successful e-KYC authentication and confirmation to resident that mobile has been re-verified

ILLUSTRATION: ANIRBAN BORA

On IVR helpline

- Resident calls the TSP IVR through the mobile number that needs to be re-verified
- IVR plays the consent message and resident provides the Aadhaar number
- OTP request sent to UIDAI if there is Aadhaar registered mobile number otherwise error message is played to the resident
- OTP is recieved on the Aadhaar registered mobile and consent message is played
- Resident enters the OTP on the IVR and e-KYC details are fetched from UIDAI
- Successful mobile re-verification message is given on IVR as well as SMS notification on subscriber's mobile

BEGINNING DEC 1 Mobile numbers can be linked with Aadhaar through websites and IVRS of telecom service providers

Playing Safe: SIM-Aadhaar Linking to be Fully Automated

Telcos will have to ensure that Aadhaar number is not accessible to customer relationship executives

Aman.Sharma@timesgroup.com

New Delhi: People will need to go to the websites of telecom service providers (TSPs) or call up their phone helplines for getting a one-time password (OTP) to link their SIM to Aadhaar from December 1, in a process that will be totally automated and without any human intervention.

These two ways of verifying one's SIM to Aadhaar have been approved by Unique Identification Authority of India (UIDAI) now. Earlier, the Department of Telecommunications (DoT) had proposed that citizens could also do the linking through OTP on sending as SMS to a number provided by the telecom operator but UIDAI did not find the same "safe", and has proposed that the linking must be done by generating an OTP either by logging onto the TSP's website or placing a call to the latter's phone helpline, a

DoT's proposal that linking be allowed through OTP received on sending SMS to a no. provided by telco rejected

senior government official told ET. Also, one needs to have a mobile number registered with Aadhaar to go through either of the two processes – or you will need to first visit an Aadhaar Centre to update your mobile number in Aadhaar records.

On the web portal, a resident will first enter the mobile number which he needs to re-verify. The TSP will generate an OTP on the entered mobile number which the person will enter on the website. "This will confirm that the mobile to be re-verified is available with the resident," as per UIDAI. A consent message, as per Aadhaar Act, will be displayed on the website and resident will enter his Aadhaar number after checking the consent box. The TSP will generate an OTP request to UIDAI and the resident will then get an OTP on the number he already has registered with Aadhaar, which he will enter to re-verify his SIM with Aadhaar. Aadhaar number entered on TSP's website will be masked and encrypted during transmission to UIDAI. The process will be similar if a person calls up the TSP's IVR helpline from the number he wish-

es to re-verify. The IVR will play a consent message to him before a person enters his Aadhaar number and then receives an OTP on his Aadhaar registered mobile number. He will subsequently enter this OTP on the IVR. "The IVR language should be in English, Hindi and other regional languages of the respective states/circles," UIDAI has said. TSPs have been asked to ensure the security of voice channels, keep the process completely automated, ensure the security provided is at par with security of banking transactions through IVR and also make sure that the application that interacts with the IVR masks or encrypts the Aadhaar number as soon as it is received by the application, for ensuring robust security and secrecy of Aadhaar number.

"TSPs will ensure that Aadhaar number is not accessible the operator's customer relationship executives," UIDAI has said. Regarding the website, operators have been asked to ensure the same is secure against known cyber-attacks and are secured through certificates. "TSP's must ensure that they have Service Engine Optimisation services for their websites and their sites feature on top during Google searches. If TSPs can provide these services through a user name and password authentication which may already exist on their websites for customers, this will further enhance the security," the UIDAI has said.