

HQ-13030/1/2022-AUTH-I HQ

भारत सरकार
भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)
अधिप्रमाणन एवं सत्यापन अनुभाग

यूआईडीएआई मुख्यालय भवन,
तृतीय तल, बंगला साहिब रोड़,
काली मंदिर के पीछे,
गोल मार्किट, नई दिल्ली - 110001
दिनांक : 10-10-2023

To,

All AUAs/KUAs

Sub: Advisory regarding improving Auth Success rate of OTP failures

Refer Letter No.-13030/1/2021-Auth-I HQ dated 20.01.2023

Dear Madam/Sir,

UIDAI has been providing Aadhaar authentication services using various modalities like Biometric (fingerprint, iris, face), OTP and demographics wherein Aadhaar number, along with other attributes (Demographics/Biometric/ OTP) is submitted to UIDAI's Central Identity Data Repository (CIDR) for verification; the CIDR verifies whether the data submitted matches the data available in CIDR and responds with a "Yes/No" or e-KYC.

2. The OTP API of UIDAI provides the definition of each error code in case of OTP authentication failure. To further explain the cause of the error codes accounting for more than 90% of failures and their remedial action an FAQ were prepared and circulated vide UIDAI letter No-13030/1/2021-Auth-I HQ dated 20.01.2023. However, based on additional observations, revised FAQ for AUA's have been prepared.

This letter supersedes UIDAI OM No-13030/1/2021-Auth-I HQ dated 20.01.2023.

Yours faithfully


(Sanjeev Yadav)
Director

Encl: Annexure-1

Copy for information to:

1. All ROs, UIDAI
2. Tech Centre, UIDAI

Annexure-1

FAQs on OTP related Error Codes

1. Error Code 400 – Invalid OTP value

This error occurs due to the following reasons;

Reason 1: Less than 6-digit, numeric value is entered by the residents.

Reason 2: Wrong numeric value (OTP) is entered.

Reason 3: Alphabets ranging from a-z are mistakenly entered.

Reason 4: Special character like #,%,&,&!,*,?,”,/,,=,+,- etc. are entered.

Reason 5: If there is no waiting time set (for re-send OTP option) at AUA or Sub-AUA application end, application allowing to generate multiple OTP in a short time spam, Failures with error-400 will be more.

Preventive Action: AUA has to develop applications where in only 6-digit numeric value will be accepted so as to overcome this error. Please extend the waiting time for OTP resend option to minimum 1 minute (60 sec-120 sec) in AUA/Sub-AUA applications. Submit OTP button should remain disabled till the time OTP API response has been received at the AUA application which will minimize the input of wrong OTP.

2. Error Code 402 - “txn” value did not match with “txn” value of Request OTP API

This error occurs due to the following reasons;

Reason 1: Due to low internet connectivity at AUA/KUA side. This can be checked from the transactional logs of AUA/KUA.

Reason 2: Due to low internet connectivity at ASA side. This can be checked from transactional logs of ASA.

Reason 3: For OTP based transactions, if the “txn” value of Auth/KYC request is not matching with the “txn” value of request OTP API then Authentication transaction will be declined with error-402.

Preventive Action: AUA have to make sure to have full internet connectivity and to resolve it, transactional logs of AUA/KUA and ASA may be checked. Please check the transaction ID setting at AUA end, txn value should be same to initiate OTP and validate OTP request.

For example - If OTP txn id is 123456 then OTP based Auth txn id should be 123456 and OTP based KYC txn id should be UKC:123456

3. Error Code 403 - Maximum number of attempts for OTP match is exceeded or OTP is not generated. Please generate a fresh OTP and try to authenticate again

This error occurs due to the following reasons;

Reason 1: If wrong value is entered more than 3 times for submission.

Reason 2: If Refresh button is used multiple times before submission.

Reason 3: If internet connectivity is low due to which OTP is not generated within the specific time period but user is trying to validate with any 6 digit number.

Reason 4: If Back button is used during the transaction, it may lead to commencement of new session in the existing session and hence, authentication will fail.

Preventive Action: Session should not be refreshed and Close/Back button should be disabled during the transaction. Enter OTP option should get enabled once OTP response has been received from UIDAI. In case-Refresh/Back button is selected, the application should logout. Please don't allow AUA application to submit OTP with blank value or with any other value if OTP response (from OTP API) is not received for that particular transaction.

4. Error Code 579 - OTP usage not allowed as per license

Reason: This error occurs when the entity doesn't have the approval related to OTP modality for performing Aadhaar authentication.

Preventive Action: The entity has to ensure whether they have sought approval for the OTP modality. If OTP modality is not active, AUA have to apply to UIDAI for activation of OTP modality.

5. Error Code 740 - Missing OTP data as specified in "Uses"

This error occurs due to the following reasons;

Reason 1: If the OTP field is left blank.

Reason 2: If complete 6-digit numeric value is not entered for submission.

Preventive Action: The OTP field can't be left blank and complete 6-digit numeric value has to be entered for submission. AUA shall make changes in the application wherein, Submit button should not be active till 6 numeric digits are fed.

6. Error Code 952 - OTP Flooding error

Reason: If multiple OTP requests initiated by the same resident in a short span of time (more than 1 OTP generation in 30 sec) 952 error will occur.

Preventive Action: Please do not allow the AUA application to generate two OTP requests within duration of 30 seconds. Please extend the waiting time for OTP resend option to minimum 1 minute (60 sec-120 sec) in AUA/Sub-AUA applications.

7. Error Code 953 - Exceeded Maximum OTP generation Limit. Max OTP generation limit is 5 (without submitting).

Reason: If resident generated 5 OTPs continuously in 30 minutes and have not submitted the OTP for validation, then the 6th attempt will be failed with error-953. OTP Generation will be blocked for certain duration (for 30 min) after exceeding the Max OTP generation limit.

Preventive Action: If error-953 comes after "Exceeded Maximum OTP generation Limit" by the resident, please populate/notify a detailed error message as mentioned above. This will prevent resident to generate the OTP for next 30 minutes.

8. Error Code 111 - Aadhaar number does not have mobile number.

Reason: If there is no mobile number linked to the Aadhaar.

Preventive Action: A static message/notification can be populated in AUA application/portal/website that "Aadhaar holder should have registered mobile number updated against their Aadhaar". For resident awareness and to avoid these OTP API failures, this message can be populated in AUA website or portal (on OTP generation page). If still resident triggering OTP and getting error-111 due to non availability of mobile in his/her Aadhaar, AUA can notify with the clear error message that "Aadhaar number does not have mobile number, to update the mobile no. in Aadhaar please visit nearest Enrollment center.

In case of any issue, AUA may contact auth-support at authsupport@uidai.gov.in

