# API 2.0 Error Handling document

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 100 | "Pi" (basic) attributes of demographic data did not match | User should be allowed to re-enter his/her personal information attributes like name, lname, gender, dob, dobt, age, phone, email whichever is used for authentication in application | Please re-enter your <name, lname, gender, dob, dobt, age, phone, email>. | Operator should re-enter correct details personal information as per the Aadhaar letter.<br>Ensure correct Aadhaar Information is entered. | One or more personal information attributes not matching. |
| 200 | "Pa" (address) attributes of demographic data did not match | User should be allowed to re-enter his/her personal address attribute like co (care of), house, street, lm (land mark), loc (locality), vtc, subdist, dist, state, pc (postal pin code), po (post office) whichever is used for authentication in application | Please re-enter your <co (care of), house, street, lm (land mark), loc (locality), vtc, subdist, dist, state, pc (postal pin code), po (post office)>. | Operator should re-enter correct details personal information as per the Aadhaar letter.<br>Ensure correct Aadhaar Information is entered. | One or more personal address attributes not matching. |
| 300 | Biometric data did not match | User should be allowed to give his finger prints "n" number of times. N should be configurable and should be set as per application requirement. (E.g. For Banking Applications it can be set at a maximum of 5 times) | Please give your finger prints again. | Ensure correct Aadhaar number is entered and try authenticating again with another finger; ensure finger is placed correctly; ensure fingers are clean; ensure finger is not very dry; ensure fingerprint scanner is clean.<br>After repeated failure, if the resident is genuine, exception handling provision would need to be followed to provide service.<br>Please contact UIDAI helpdesk to inform about the issue and to understand the steps for the updation of the biometric information in CIDR. | Finger print is not given properly, scanner has some dust accumulated, fingers were wet, position of finger not appropriate, scanned finger NFIQ not good |
| 310 | Duplicate fingers used | Application should prompt user to try again with distinct fingers. | Please try again with distinct fingers. | Operator should insure that the resident is providing distinct fingers (two different fingers) for "two finger" authentication. | Error occurs when same finger is sent as two or more separate records within same request. For two-finger auth, if resident puts same finger again, then this happens. |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 311 | Duplicate Irises used | Application should prompt user to try again with distinct irises. | Please try again with distinct irises. | Operator should ensure that the resident is providing distinct irises (two different irises) for authentication. | Error occurs when same iris is sent as two or more separate records within same request. |
| 312 | FMR and FIR cannot be used in same transaction | Application should ensure that authentication request does not mix FMR and FIR in the same transaction e.g. in case of two finger authentication, data for two distinct fingers should either be sent in FMR format or in FIR format. | Technical Exception <No> | Contact technical helpdesk. | Auth packet cannot mix fingerprint "image" records (FIR) and fingerprint "minutiae" records (FMR). AUA app should choose either one or another. FMR is recommended. |
| 313 | Single FIR record contains more than one finger | Application should prompt user to try again by placing single finger. | Please try again by placing Single finger on the authentication device. | Operator should ensure that the resident is providing single finger for authentication. | As per ISO spec, one FIR can contain one or more finger images within itself (like slap, etc). UIDAI currently supports single finger record only. If there is a requirement to send 2 fingers, 2 different biometric records should be sent. |
| 314 | Number of FMR/FIR should not exceed 10 | Application should ensure that one auth request should not contain more than 10 FMR/FIR records. | | | Auth Request has more than 10 finger records |
| 315 | Number of IIR should not exceed 2 | Application should ensure that one auth request should not contain more than 2 IIR records. | | | Auth Request has more than 2 iris records |
| 316 | Number of FID should not exceed 1. | The biometric data is of type “Face Image Data”, application must ensure that one auth request should contain only one face image data | | | Auth request has more than one " Face image Data " |
| 330 | Biometrics locked by Aadhaar holder | Resident has securely locked his Biometrics | | Resident has locked his biometrics , he can invoke Resident portal or M-Aadhaar and get his biometric unlocked and get himself authenticated | Resident can go to uidai resident portal or maadhaar and get his biometrics unlocked and get himself authenticated |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 400 | "OTP" validation failed | Application should have provision for allowing user to provide OTP value again and after some retries (configurable) option to generate OTP again. | Please provide correct OTP value. | If there are repeated failures user is advised to generate new OTP and send the authentication request using the new OTP. | Incorrect OTP value is entered. Input not matching with the value in CIDR. |
| 402 | “txn” value did not match with “txn” value used in Request OTP API. | Authenticator specific transaction identifier. Application must ensure that in case of OTP based Auth transaction the "txn" must be exactly the same as was used during OTP request | Technical Exception <> | AUA application must ensure that in case of OTP based authentication the "txn" must be the same as was used while otp generation. | The transaction "txn" passed in auth verify call doesnot match with the "txn" that was used during OTP request generation. |
| 500 | Invalid Skeyencryption | Application should not have hard coded digital certificate information. It should be configurable. | Note: Application can throw Auth API error code number on screen. So that contact centre or application support helpline can understand the reason. | Please contact authsupport team of UIDAI | Use of wrong digital certificate for encryption of AES-256 Key (session key). |
| 501 | Invalid value for "ci" attribute in "Skey" element | Application should not have hard coded "ci" attribute value. It should be configurable. | Technical Exception <> | | Ensure that expiry date of UIDAI certificate used for encryption of Skey is specified as "ci" value. |
| 502 | Invalid Pid Encryption | Application should do extensive testing using UIDAI Test Auth Service to ensure compliance with auth API. | Technical Exception <No> | | Ensure that correct AES encryption has been used.<br>Ensure that AES key used for encryption of "Pid" XML was encrypted and specified as value for Skey. |
| 503 | Invalid HMac encryption | Application should do extensive testing using UIDAI Test Auth Service to ensure compliance with auth API. | Technical Exception <No> | | Ensure that correct AES encryption has been used.<br>Ensure that AES key used for encryption of "Hmac" was encrypted and specified as value for Skey.<br>Ensure that same AES key is used for encryption of Pid and Hmac. |
| 504 | Session key re-initiation required due to expiry or key out of sync | Application should have a provision to send full session key and initiate a new session in case of such failure. | Technical Exception <No> | Please try again. | When Synchronized Session Key scheme is used, this can happen if either session is expired (currently configured to max 4 hrs) or if the key goes out of sync. |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 505 | Synchronized Skey usage is not allowed | Application should use full skey | Technical Exception <No> | Switch to full skey scheme | This happens when AUA does not have privilage to use SSK scheme |
| 510 | Invalid Auth XML format | Application Authentication request should comply to Authentication API latest version and application should validate its structure before sending it to CIDR for authentication. | Technical Exception <No> | Please ensure that the latest recommended API is used for application development. Refer UIDAI website for the latest version of API.<br>If this does not resolve the issue than please contact technical helpdesk. | Non compliance with supported Authentication API version structure in CIDR. |
| 511 | Invalid PID XML format | Application Authentication request should comply to PID XML format defined in Authentication API latest version and structural validation should be done before encryption of PID XML. | Technical Exception <No> | Please ensure that the latest recommended API is used for application development. Refer UIDAI website for the latest version of API.<br>If this does not resolve the issue than please contact technical helpdesk. | Non compliance with supported Authentication API version structure in CIDR. |
| 512 | Invalid Aadhaar holder consent in “rc” attribute of “Auth” | Aadhaar holder consent to do the Aadhaar based authentication using OTP or Biometrics. Only allowed value is “Y”. | | Without explicit informed consent of the Aadhaar holder AUA/Sub-AUA application should not call this API | "rc" is a mandatory attribute . AUA /sub-AUA application must ensure to have an explicit concent from the aadhaar holder before making an API call. |
| 513 | Invalid Protobuf Format | Incorrect Binary format of the PID Block | Technical Exception <No> | | Application must verify the protobuf format being used for PID creation |
| 520 | Invalid “tid” value | In case of Registered devices, value should be passed as “registered” for all biometric based authentication and value for the attribute “” in case of a non biometric based transaction. | Technical Exception <No> | | In case of Auth API 2.0 registered device specification the "tid" attribute must “**registered**” for all biometric based authentication and value for the attribute **“”** in case of a non biometric based transaction. The value must be all lower case, no spaces or special char else will result in this error. |
| 521 | Invalid “dc” code under Meta tag | "dc" is a mandatory attribute for biometric based auth Unique Registered Device Code. " dc" is returned by RD Service when using biometric authentication | Technical Exception <No> | | Application should obtain proper device code from the certified RD service and use the same for biometric based authentication., non valid or non registered devie would result in the |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| | | | | | same error |
| 524 | Invalid “mi” code under Meta tag | "mi" Model Id is a mandatory attribute for biometric based auth as part of Registered device specification . Returned by RD Service when using biometric authentication. | Technical Exception <No> | | Application should obtain proper "mi" Model Id details from the certified RD service and use the same for biometric based authentication., non valid or non registered device model would fail with same error |
| 527 | Invalid “mc” code under Meta tag. | "mc" attribute holds registered device public key certificate. This is signed with device provider key. Returned by RD Service when using biometric authentication. | Technical Exception <No> | | Application must ensure that a valid "mc" is used in the request and is signed by device provider key . A wrong "mc" passed in the request would result in same error |
| 528 | Device - Key Rotation policy | The device certificate used in the request is not meeting the UIDAI key rotation policy guidelines . | Technical Exception <No> | Please contact authsupport team of UIDAI | The Device certificate used the API request is not meeting the UIDAI key rotation policy guidelines |
| 530 | Invalid authenticator code | Application should pass valid AUA code in authentication request which is registered with UIDAI. Value of this code should be configurable. | Technical Exception <No> | | AUA code used in Authentication request is not valid.<br>or<br>AUA code used in the Auth URL is not same as the AUA code used in the Auth XML. |
| 540 | Invalid Auth XML version | Application should pass supported valid API version in authentication request. Value of this should be configurable. | Technical Exception <No> | | API version used in Auth XML (Authentication request) is either not supported or invalid. |
| 541 | Invalid PID XML version | Application should pass supported valid API PID XML version in authentication request. Value of this should be configurable. | Technical Exception <No> | | Version of the "Pid" element used<br>In the PID XML (Authentication request) is either not supported or invalid. |
| 542 | AUA not authorized for ASA. | Application should ensure link is in place between AUA-ASA before sending request to CIDR. | | Ensure the authentication request is being sent through the authorized ASA as per the records of UIDAI.<br>or | This error will be returned if AUA and ASA do not have linking in the portal |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| | | | | Please contact UIDAI helpdesk to report the issue and to understand further steps for the updation of ASA-AUA linkage. | |
| 543 | Sub-AUA not associated with "AUA" | Application should ensure Sub-AUA is added and associated with correct AUA before sending request to CIDR. | | Ensure the authentication request is being sent through the associated AUA as per the records of UIDAI.<br>or<br>Please contact UIDAI helpdesk to report the issue and to understand further steps for the updation of ASA-AUA linkage. | This error will be returned if Sub-AUA specified in "sa" attribute is not added as "Sub-AUA" in portal |
| 550 | Invalid "Uses" element attributes | Application should use valid attributes defined in API for <Uses> tag and validation on Auth request should be done before sending request to CIDR. | Technical Exception <No> | | Invalid attributes used in Uses tag.<br>This error is typically reported if "bt" attribute has been specified but bio="n" in Uses element. "bt" attribute is required only if bio="y" in Uses element. |
| 552 | WADH Validation failed | "WADH" - Wrapper API data hash , SHOULD BE empty for all regular authentication transactions and must be ONLY used for specific transaction types such as eKYC and Update APIs. We can also result in similar error in case of WADH validation failure from auth side | Technical Exception <No> | | AUA application must ensure that the "WADH" attribute is passed empty for all regular authentication transactions and used ONLY for wrapper API transaction calls such as eKYC and Update APIs.<br>Bug in AUA Application can also result in similar error and result with WADH validation failure |
| 553 | Registered devices currently not supported. This feature is being implemented in a phased manner. | Returned when the registered device services are not supported . Request you to get in touch with Athsupport team | Technical Exception <No> | | Returned when the registered device services are not supported . Request you to get in touch with Athsupport team |
| 554 | Public devices are not allowed to be used | Returned when the public devices are not supported by the API or completely faced out from the UIDAI ecosystem . | Technical Exception <No> | | Returned when the public devices are not supported by the API or completely faced out from the UIDAI ecosystem . Request you to get in touch with |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| | | Request you to get in touch with Athsupport team | | | Athsupport team |
| 555 | rdsId is invalid and not part of certification registry | "rdsid" Registered Device Service ID. The application should input a valid rdsid which is certified and listed in registry xml and passed in the request . This attribute is mandatory for biometric based transactions. If the registered devices service is not used, the value for the attribute can be NA or else the attribute itself may not part of the request xml | Technical Exception <No> | | AUA application should input a valid **rdsid** which is certified and listed in registry xml and passed in the request . This attribute is mandatory for all biometric based transaction and If the registered devices service is not used, the value for the attribute can be NA or else the attribute itself may not part of the request xml |
| 556 | rdsVer is invalid and not part of certification registry. | "rdsVer" Registered Device Service Version . The application should input a valid "**rdsVer**" which is certified and listed in registry xml and passed in the request . This attribute is mandatory for biometric based transactions. If the registered devices service is not used, the value for the attribute can be NA or else the attribute itself may not part of the request xml | Technical Exception <No> | | AUA application should input a valid **rdsVer** which is certified and listed in registry xml . This attribute is mandatory for all biometric based transaction and If the registered devices service is not used, the value for the attribute can be NA or else the attribute itself may not part of the request xml |
| 557 | dpId is invalid and not part of certification registry. | "dpid" Registered Device Provider ID . The application should input a valid "**dpid**" which is certified and listed in registry xml . This attribute is mandatory for biometric based transactions. If the registered devices service is not used, the value for the attribute can be NA or else the attribute itself may not part of the request xml | Technical Exception <No> | | AUA application should input a valid **dpid** which is certified and listed in registry xml . This attribute is mandatory for all biometric based transaction and If the registered devices service is not used, the value for the attribute can be NA or else the attribute itself may not part of the request xml |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 558 | Invalid dih | "dih" Device Info Hash is a mandatory attribte and has to be calculated by Registered Device (RD) service during the PID block capture when using biometrics | Technical Exception <No> | | "dih" Device Info Hash is a mandatory attribte and has to be calculated by Registered Device (RD) service during the PID block capture when using biometrics |
| 559 | Device Certificate has expired | Application should use a valid device certificate, this error is reported when the validity of the device certificate is expired | Technical Exception <No> | | Application should use a valid device certificate, this error is reported when the validity of the device certificate is expired. Please contatct the device provider |
| 560 | DP Master Certificate has expired | Application should use a valid device provider certificate, the subject error is reported when the validity of the device provider certificate is expired | Technical Exception <No> | | Application should use a valid device provider certificate, the subject error is reported when the validity of the device provider certificate is expired, please contatct the device provider |
| 561 | Request expired ("Pid->ts" value is older than N hours where N is a configured threshold in authentication server) | AUA application should not store Pid block and in case of application which are using thick client there should be a provision to sync up date with server at start. | 1. In case of Device/Client based Application<br>a. Either device date/time is behind current date/time or request is old. Please try again.<br>2. In case of web based Application<br>a. Technical Exception <No> | Please verify that the device/client date/time is synchronised with Indian Standard Time (IST) and resend the authentication request. | Either Device/Client/Server date/time is behind current one or old stored pid is getting sent. |
| 562 | Timestamp value is future time (value specified "Pid->ts" is ahead of authentication server time beyond acceptable threshold) | AUA application should not store Pid block and in case of application which are using thick client there should be a provision to sync up date with server at start. | 1. In case of Device/Client based Application<br>a. Either device date/time is ahead current date/time or request is old. Please try again.<br>2. In case of web based Application<br>a. Technical Exception <No> | Please verify that the device/client date/time is synchronised with Indian Standard Time (IST) and resend the authentication request. | Device/Client/server date/time is ahead than current date/time. |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 563 | Duplicate request (this error occurs when exactly same authentication request was re-sent by AUA) | Application should ask user to try again. | Please submit your request again. | User is required to send the authentication request once again. | If same "Auth XML" is sent more than once to server, then, 2nd and subsequent requests will fail with this error. |
| 564 | HMAC Validation failed | Application should create HMAC using *SHA-256* | Technical Exception <No> | | HMAC is not calculated using API defined algorithm |
| 565 | AUA License key has expired | Application should have a configurable License key management feature through which one can manage Key without changing application. | Technical Exception <No> | | Current AUA License has expired. |
| 566 | Invalid non-decryptable license key | The licence key used is not decryptable | Technical Exception <No> | | License key used in application is invalid. |
| 567 | Invalid input (this error occurs when some unsupported characters were found in Indian language values, "lname" or "lav") | Application should have client/server level checks to stop users to input unsupported characters. | Technical Exception <No> | | some unsupported characters were found in Indian language values, "lname" or "lav" in Auth request XML |
| 568 | Unsupported Language | Application should have client/server level checks to restrict users to only select language from API supported local Language. | Technical Exception <No> | | Value of "lang" attribute is not from the list supported by authapi. |
| 569 | Digital signature verification failed (this means that authentication request XML was modified after it was signed) | Application should ensure security of data end to end ie. From client/device to CIDR server by using appropriate communication protocol. | Technical Exception <No> | | Authentication request XML was modified after it was signed. |
| 570 | Invalid key info in digital signature (this means that certificate used for signing the authentication request is not valid – it is either expired, or does not belong to the AUA or is | Application should have an independent module for signing Auth XML and certificate should be stored and manage outside of the application. | Technical Exception <No> | | Certificate used for signing the authentication request is not valid – it is either expired, or does not belong to the AUA or is not created by a well-known Certification Authority |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| | not created by a well-known Certification Authority) | | | | |
| 571 | PIN Requires reset (this error will be returned if resident is using the default PIN which needs to be reset before usage) | | Please reset your PIN in UIDAI updation application and use new PIN in this application. | Please change your default PIN through UIDAI updation client and resend your authentication request. | This error will be returned if resident is using the default PIN which needs to be reset before usage. |
| 572 | Invalid biometric position (This error is returned if biometric position value - "pos" attribute in "Bio" element - is not applicable for a given biometric type - "type" attribute in "Bio" element.) | Application should have client level validation to check "type" and corresponding valid "pos" values before creating PID block. | Technical Exception <no> | | This error is returned if biometric position value - "pos" attribute in "Bio" element - is not applicable for a given biometric type - "type" attribute in "Bio" element |
| 573 | Pi usage not allowed as per license | Application should have a configurable business rule which can restrict the usage of Pi attribute based on AUA license authorization. | Technical Exception <No> | | Pi usage not allowed as per license |
| 574 | Pa usage not allowed as per license | Application can have a client level check to restrict/allow entry of "pa" attribute as per license of AUA. | Technical Exception <No> | | Pa usage not allowed as per license |
| 575 | Pfa usage not allowed as per license | Application can have a client level check to restrict/allow entry of "pfa" attribute as per license of AUA. | Technical Exception <No> | | Pfa usage not allowed as per license |
| 576 | FMR usage not allowed as per license | Application can have a client level check to restrict/allow entry of "FMR" attribute as per license of AUA. | Technical Exception <No> | | FMR usage not allowed as per license |
| 577 | FIR usage not allowed as per license | Application can have a client level check to restrict/allow entry of "FIR" attribute as per license of AUA. | Technical Exception <No> | | FIR usage not allowed as per license |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 578 | IIR usage not allowed as per license | Application can have a client level check to restrict/allow entry of "IIR" attribute as per license of AUA. | Technical Exception <No> | | IIR usage not allowed as per license |
| 579 | OTP usage not allowed as per license | Application can have a client level check to restrict/allow entry of "OTP" attribute as per license of AUA. | Technical Exception <No> | | OTP usage not allowed as per license |
| 580 | PIN usage not allowed as per license | Application can have a client level check to restrict/allow entry of "PIN" attribute as per license of AUA. | Technical Exception <No> | | PIN usage not allowed as per license |
| 581 | Fuzzy matching usage not allowed as per license | Application can have a client level check to restrict/allow entry of "ms" attribute in pi, pa and pfa element as per license of AUA. | Technical Exception <No> | | Fuzzy matching usage not allowed as per license |
| 582 | Local language usage not allowed as per license | Application can have a client level check to restrict/allow entry of local language attribute in pi, pa and pfa element as per license of AUA. | Technical Exception <No> | | Local language usage not allowed as per license |
| 586 | FID usage not allowed as per license. | FID usage not allowed as per license. This feature is being implemented in a phased manner | Technical Exception <No> | Please contact authsupport team of UIDAI | FID usage not allowed as per license. This feature is being implemented in a phased manner. |
| 587 | Name space not allowed. | Name space usage is allowed for wrapper API applications like eKYC ,MOU etc | Technical Exception <No> | | Name space usage is allowed for wrapper API applications like eKYC ,MOU etc |
| 588 | Registered device not allowed as per license | The licence key used doesn't support usage of Registered devices services, contact Auth support and get the new lincencekey generated that supports registered device services | Technical Exception <No> | Please contact authsupport team of UIDAI | The licence key used doesn't support usage of Registered devices services, contact Auth support and get the new lincencekey generated that supports registered device services |
| 590 | Public device not allowed as per license. | Usage of Public devices not allowed as per the Licence provided | Technical Exception <No> | Please contact authsupport team of UIDAI | Usage of Public devices not allowed as per the Licence provided |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 710 | Missing "Pi" data as specified in "Uses" | Application should validate pid block before encrypting data with API specified PID block structure and "Uses" element attributes values to ensure PID block have all the elements and attributes. Client level validation should also be put to check all mandatory and conditional fields of API XML. | Technical Exception <No> | | Missing "Pi" data as specified in "Uses" |
| 720 | Missing "Pa" data as specified in "Uses" | Same as 710 | Technical Exception <No> | | Missing "Pa" data as specified in "Uses" |
| 721 | Missing "Pfa" data as specified in "Uses" | Same as 710 | Technical Exception <No> | | Missing "Pfa" data as specified in "Uses" |
| 730 | Missing PIN data as specified in "Uses" | Same as 710 | Technical Exception <No> | | Missing PIN data as specified in "Uses" |
| 740 | Missing OTP data as specified in "Uses" | Same as 710 | Technical Exception <No> | | Missing OTP data as specified in "Uses" |
| 800 | Invalid biometric data | AUA to review biometric device being used and whether templates are ISO compliant. | Technical Exception <No> | | FMR value is not ISO compliant – bad header or other issue with templates.<br>FIR/IIR value is not compliant, or templates could not be extracted for the given FIR/IIR for matching purposes. |
| 810 | Missing biometric data as specified in "Uses" | Same as 710 | Technical Exception <No> | | Missing biometric data as specified in "Uses" |
| 811 | Missing biometric data in CIDR for the given Aadhaar number | | Your Biometric data is not available in CIDR. | Ensure correct Aadhaar number is entered and try authenticating again.<br><br>After repeated failure, if the resident is genuine, exception handling provision would need to be followed to provide service. | AUAapplication must ensure that the correct aadhaar number isused while transacting.<br>In case of repeated failures and if the resident is genuine , exception handling mechanism must be followed to provide service to resident. |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| | | | | Please contact UIDAI helpdesk to inform about the issue and to understand the steps for the updation of biometric information in CIDR. | |
| 812 | Resident has not done "Best Finger Detection". Application should initiate BFD application to help resident identify their best fingers. See Aadhaar Best Finger Detection API specification. | Application should make provison to initiate BFD API call to help Aadhaar holder to identify their best fingers. | You have not done best finger detection so kindly proceed with the BFD process for successful authentication. | Refer Aadhaar Best Detection API specifications for details on the BFD process. | Resident has not done "Best Finger Detection". |
| 820 | Missing or empty value for "bt" attribute in "Uses" element | Same as 710 | Technical Exception <No> | | Missing or empty value for "bt" attribute in "Uses" element |
| 821 | Invalid value in the "bt" attribute of "Uses" element | Same as 710 | Technical Exception <No> | | Invalid value in the "bt" attribute of "Uses" element |
| 822 | Invalid value in the “bs” attribute of “Bio” element within “Pid” | AUA application should call the registered device capture function to obtain the bio record as well as the signature string (bs). "bs" is Base-64 encoded signed biometric hash of the bio record | | | "bs" is Base-64 encoded signed biometric hash of the bio record and formed by invoking the RD services during the biometric capture method, if the bs validation fails the error is resulted |
| 901 | No authentication data found in the request (this corresponds to a scenario wherein none of the auth data – Demo, Pv, or Bios – is present) | Application should validate that User giveatleast one auth factor before encryption of PID block. | Technical Exception <No> | | All factors of Auth are optional. Hence, it is possible to attempt an auth without specify any values for any of the factors – Pi, Pa, Pfa, Bio or Pv. If none of these elements have any value that can be used for authentication purposes, then, this error will be reported. |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 902 | Invalid "dob" value in the "Pi" element (this corresponds to a scenarios wherein "dob" attribute is not of the format "YYYY" or "YYYY-MM-DD", or the age of resident is not in valid range) | Application should have a client level check to check dob date format and age business rules specified (Current Rule is that age should not be less than 0 and greater than 150 years) | Please enter dob in specified date format or enter age in specified range. | Re-enter the date of birth or age and resend a new authentication request. | "dob" attribute is not of the format "YYYY" or "YYYY-MM-DD", or the age of resident is not in valid range. |
| 910 | Invalid "mv" value in the "Pi" element | Same as 710 | Technical Exception <No> | | |
| 911 | Invalid "mv" value in the "Pfa" element | Same as 710 | Technical Exception <No> | | |
| 912 | Invalid "ms" value | Same as 710 | Technical Exception <No> | | |
| 913 | Both "Pa" and "Pfa" are present in the authentication request (Pa and Pfa are mutually exclusive) | Same as 710 | Technical Exception <No> | | Attempt to use Pa and Pfa both in the same request can result in this error. |
| 930-939 | Technical error that are internal to authentication server | AUA/ASA should call UIDAI tech support. | Technical Exception <No> | | UIDAI server side issues. UIDAI tech support to review the scenario and take appropriate action. |
| 940 | Unauthorized ASA channel | AUA should consult ASA. | Technical Exception <No> | | |
| 941 | Unspecified ASA channel | AUA should consult ASA. | Technical Exception <No> | | |
| 950 | OTP store related technical error | No action required contact auth support | Technical Exception <No> | | No action required contact auth support |
| 951 | Biometric lock related technical error | No action required contact auth support | Technical Exception <No> | | No action required contact auth support |
| 980 | Unsupported option | AUA to review the auth client to check whether any dev feature is being used in prod | Technical Exception <No> | | Currently this error is not reported. Can be used in future. |
| 995 | Aadhaar suspended by competent authority | No action required contact auth support | | | No action required contact auth support |

| API Error Code | Description | Provision Required in the Application | Suggested Message to the User | Suggested instructions to the user | Probable Reasons |
|---|---|---|---|---|---|
| 996 | Aadhaar Cancelled ( Aadhaar is not in authenticable status ) | AUA Application must consume the ACTN attribute of the API response , ACTN attribute provides necessary feedback to the end AUA/resident on the next action. | Resident should re-enroll. | | Aadhaar is not in authenticable status.<br>**Please see ACTN attribute in response for actionable by the resident. |
| 997 | Aadhaar Suspended ( Aadhaar is not in authenticable status ) | AUA application should have mechanism to handle this scenario as Aadhaar number is valid but its status is not active. | Your Aadhaar number status is not active. Kindly contact UIDAI Helpline. | | Aadhaar is not in Auhenticatable status.<br>**Please see ACTN attribute in response for actionable by the resident. |
| 998 | Invalid Aadhaar Number 0r Non Availability of Aadhaar data | AUA application should have a client level validation for Aadhaar number validity ie. should be 12 digits and conform to Verhoeff algorithm. | Ensure you have entered correct Aadhaar number. Please retry with correct Aadhaar number after sometime. | Ensure you have entered correct Aadhaar number. Please retry with correct Aadhaar number after sometime. | If client level validations are done then Aadhaar number does not exist in CIDR. Please retry with correct Aadhaar number after sometime.<br>**Please see ACTN attribute in response for actionable by the resident. |
| 999 | Unknown error | No action required contact auth support | Technical Exception <No> | Please contact authsupport team of UIDAI | |