How to handle Aadhaar Authentication Issues during operation of PoS device

Error Handling

This page provides guidelines for handling PoS Application Programming Interface (API) errors within the application. While developing applications, AUAs need to decide how to handle the errors gracefully and provide resident/operator friendly messages. Simply showing the error on screen is not helpful. This document is an attempt to provide guidelines for doing better error handling.

Following table describes API error codes, suggestion for how to handle it, possible message to user, and probable reasons for the error.

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. 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. 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	Please give your finger prints again.	Ensure correct Aadhaar number is entered and try authenticating again with	Finger print is not given properly, scanner has some dust accumulated, fingers were wet,

		configurable and should be set as per application requirement. (E.g. For Banking Applications it can be set at a maximum of 5 times)		another finger; ensure finger is placed correctly; ensure fingers are clean; ensure finger is not very dry; ensure fingerprint scanner is clean. After repeated failure, if the resident is genuine, exception handling provision would need to be followed to provide service. Please contact UIDAI helpdesk to inform about the issue and to understand the steps for the updation of the biometric information in CIDR.	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.
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,	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

		data for two distinct fingers should either be sent in FMR format or in FIR format.			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
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.
401	"Tkn" validation failed	Application should derive the value of tkn (currently only mobile number) from network. This element is meant for self-service transations on mobile (SMS/USSD, etc) where AUA derives the mobile number from the network provider and passes it on as part of API to use it as a factor.			Provided "Tkn" details are not matching with registered values in CIDR.

500	Invalid Skeyencryption	Application should not have hard coded digital certificate information. It should be configurable.	Technical Exception <No> Note: Application can throw Auth API error code number on screen. So that contact centre or application support helpline can understand the reason.	Contact technical helpdesk.	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. 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. Ensure that AES key used for encryption of "Hmac" was encrypted and specified as value for Skey. 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.

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. 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. If this does not resolve the issue than please contact technical helpdesk.	Non compliance with supported Authentication API version structure in CIDR.
520	Invalid device	Application should ensure that “tid” attribute in Auth XML has value “public”	Technical Exception <No>		Using any other value other than “public” (all lower case, no spaces or special char) will result in this error.
521	Invalid Finger device (fdc in Meta element)	Application should obtain proper code from fingerprint sensor vendor and use it	Technical Exception <No>		FDC codes are assigned as part of certification and application developer should use proper fdc code given by the fingerprint sensor/extractor vendor

522	Invalid Iris device (idc in Meta element)	Application should obtain proper code from iris sensor vendor and use it	Technical Exception <No>		IDC codes are assigned as part of certification and application developer should use proper idc code given by the iris sensor/extractor vendor
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. or 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 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. or 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 AUA and ASA do not have linking in the portal

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. or 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. 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.
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 a. Either device date/time is behind current date/time or request is old. Please try again. 2. In case of web based Application 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	AUA application should not	1. In case of	Please verify that the	Device/Client/server date/time is

	time (value specified "Pid->ts" is ahead of authentication server time beyond acceptable threshold)	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.	Device/Client based Application a. Either device date/time is ahead current date/time or request is old. Please try again. 2. In case of web based Application a. Technical Exception <No>	device/client date/time is synchronised with Indian Standard Time (IST) and resend the authentication request.	ahead than current date/time.
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	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 License has expired.
566	Invalid license key	Application should have a License key management feature through which one can manage Key without changing application.	Technical Exception <No>		License key used in application is invalid.
567	Invalid input (this error	Application should have	Technical Exception		some unsupported characters

	occurs when some unsupported characters were found in Indian language values, "lname" or "lav")	client/server level checks to stop users to input unsupported characters.	<No>		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 not created by a well-known Certification Authority)	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
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"	Application should have client level validation to check "type" and corresponding valid "pos" values before creating PID	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"

	element - is not applicable for a given biometric type - "type" attribute in "Bio" element.)	block.			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
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	Application can have a client	Technical Exception		OTP usage not allowed as per

	per license	level check to restrict/allow entry of "OTP" attribute as per license of AUA.	<No>		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
584	Invalid Pin code in Meta element	Pincode should have a valid value (in lov attribute)	Technical Exception <No>		If pincode value is not one of the valid values in UIDAI system, this error occurs
585	Invalid Geo code in Meta element	Geo code value must be a valid lat.long value in decimal format as per spec (in lov attribute)	Technical Exception <No>		If geo code does not have proper format as per spec (decimal representation with porecision upto 4 decimal values for lat and long), this error occurs
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	Technical Exception <No>		Missing "Pi" data as specified in "Uses"

		validation should also be put to check all mandatory and conditional fields of API XML.			
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. 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. After repeated failure, if the resident is genuine, exception handling provision would need to	

				be followed to provide service. 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 application based on the error code to help resident 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
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.

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			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>		

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.
996	Aadhaar Cancelled		Resident should re-enroll.		Aadhaar is no in authenticable status. **Please see ACTN attribute for actionable by the resident.
997	Aadhaar Suspended	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. **Please see ACTN attribute 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. **Please see ACTN attribute for actionable by the resident.
999	Unknown error		Technical Exception <No>	Please contact authsupport team of UIDAI	

****ACTN Codes**

Error Code	ACTN	Actionable Message
996	A401	Aadhaar cancelled being a duplicate. Resident shall use valid Aadhaar.
996	A402	Aadhaar cancelled due to disputed enrolment. Shall re-enrol if resident doesn't have a valid Aadhaar.
996	A403	Aadhaar cancelled due to technical Issues. Resident shall contact UIDAI contact centre.
996	A404	Aadhaar cancelled due to disputed enrolment (BE). Shall re-enrol if resident doesn't have a valid Aadhaar.
996	A405	Aadhaar cancelled due to errorneous enrolment (Iris). Shall re-enrol if resident doesn't have a valid Aadhaar.
997	A301	Aadhaar suspended due to inactivity. Resident shall follow the Reactivation process.
997	A302	Aadhaar suspended due to Biometrics integrity issue. Resident shall visit Permanent Enrolment Centre with document proofs for update.
997	A303	Aadhaar suspended due to Demographic integrity issue. Resident shall visit Permanent Enrolment Centre / UIDAI website with document proofs for update.
997	A304	Aadhaar suspended due to Address dispute. Resident shall visit Permanent Enrolment Centre with document proofs for update.
997	A305	Aadhaar suspended due to Photo dispute. Resident shall visit Permanent Enrolment Centre with document proofs for update.
997	A306	Aadhaar suspended due to Age dispute. Resident shall update the age.
997	A307	Aadhaar suspended since child has not updated biometrics after age of 5. Resident shall update the biometrics.
997	A308	Aadhaar suspended since resident has not updated biometrics after age of 15. Resident shall update the biometrics.
997	A309	Aadhaar is locked by resident. Resident shall follow the Un-locking process.
998	A201	Aadhaar number is incorrect. Resident shall use correct Aadhaar.
998	A202	Authentication temporarily not available, resident shall retry after sometime.

KYC related Error Codes and Description

KYC API can return following error codes in the response in case of failures:
Error code Description

S. No.	Error Codes	Reason for Error
1.	K100	Resident authentication failed
2.	K200	Resident data currently not available
3.	K540	Invalid KYC XML
4.	K541	Invalid KYC API version
5.	K542	Invalid resident consent (“rc” attribute in “Kyc” element)
6.	K543	Invalid timestamp (“ts” attribute in “Kyc” element)
7.	K544	Invalid resident auth type (“ra” attribute in “Kyc” element)
8.	K545	Resident has opted out of this service
9.	K550	Invalid “Uses” element attributes – must have either bio or otp enabled for resident authentication
10.	K551	Invalid “Txn” namespace (should be “UKC”)
11.	K552	Invalid license key
12.	K569	Digital signature verification failed for KYC XML (means that authentication request XML was modified after it was signed)
13.	K570	Invalid key info in digital signature for KYC XML (it is either expired, or does not belong to the KUA or is not created by a well known Certification Authority)
14.	K600	AUA is invalid or not an authorized KUA
15.	K601	ASA is invalid or not an authorized KSA
16.	K602	KUA encryption key not available
17.	K603	KSA encryption key not available
18.	K604	KSA not allowed to sign
19.	K999	Unknown error
20.	K955	Technical error
21.	N - 100	This is the exception happening when the ASA get the request and there is some error in the request. The description of the error is shared with AUA along with the error
22.	P- 109	This is socket timeout exception between ASA server and UIDAI’s CIDR. This happens when no response is received from UIDAI
23.	X - 666	This error is reported when ASA is not able to connect to UIDAI server
24.	X- 888	This error is reported when UIDAI sends back a blank response
25.	C - 100	It has been observed that in these cases the xml sent is invalid

Abbreviations used:

S. no.	Abbreviation	Full Form
1.	UIDAI	Unique Identification Authority of India
2.	KYC	Know Your Customer
3.	AUA	Aadhaar Authentication User Agency
4.	ASA	Authentication Service Agency
5.	CIDR	Central Identities Data Repository
6.	NIFQ	NIST Fingerprint Image Quality
7.	NIST	National Institute of Standards and Technology
8.	FMR	Fingerprint Minutiae Record
9.	FIR	Fingerprint Image Record
10.	IIR	Iris Image Record
11.	FDC	Fingerprint device code
12.	IDC	Iris device code
13.	HMAC	Hash-based Message Authentication Code