

AUA ERROR CODES

Error Code	Short Description	Description	Action Code	Action	Probable Reasons
100	Pi Mismatch	"Pi" (basic) attributes of demographic data did not match			One or more personal information attributes not matching.
110	Aadhaar number does not have verified mobile/email				
111	Aadhaar number does not have verified mobile			Mobile number registration is available on UIDAI portal as well as through the Mobile Update service	
112	Aadhaar number does not have both email and mobile.				
200	Pa Mismatch	"Pa" (address) attributes of demographic data did not match			One or more personal address attributes not matching.
300	Bio Mismatch	Biometric data did not match			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 Finger	Duplicate fingers used			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 Iris	Duplicate Irises used			Error occurs when same iris is sent as two or more separate records within same request.
312	Mixed FIR FMR	FMR and FIR cannot be used in same transaction			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	FIR Finger Exceeded	Single FIR record contains more than one finger			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	FIR Record Exceeded	Number of FMR/FIR should not exceed 10			Auth Request has more than 10 finger records
315	IIR Record Exceeded	Number of IIR should not exceed 2			Auth Request has more than 2 iris records
316	FID Record exceeded	Number of FID should not exceed 1.			
330	Biometrics Locked	Resident has locked biometrics to disable biometric authentication.			User can authenticate using biometrics only after unlocking the biometrics or Disable the biometric locking feature.
400	OTP Validation Failed	"OTP" validation failed			Incorrect OTP value is entered. Input not matching with the value in CIDR.
401	TKN Validation Failed	"Tkn" validation failed			Provided "Tkn" details are not matching with registered values in CIDR.
402	"txn" value did not match with "txn" value used in Request OTP API	"txn" value did not match with "txn" value used in Request OTP API			
500	Invalid Skey Encryption	Invalid Skeyencryption			Use of wrong digital certificate for encryption of AES-256 Key (session key).
501	Invalid ci Attribute	Invalid value for "ci" attribute in "Skey" element			Ensure that expiry date of UIDAI certificate used for encryption of Skey is specified as "ci" value.
502	Invalid Pid Encryption	Invalid Pid Encryption			Ensure that correct AES encryption has been used. 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.

503	Invalid HMAC Encryption	Invalid HMac encryption			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	Unsynced Session Key	Session key re-initiation required due to expiry or key out of sync			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 Disallowed	Application should use full skey			This happens when AUA does not have privilege to use SSK scheme
510	Invalid Auth XML	Invalid Auth XML format			Non-compliance with supported Authentication API version structure in CIDR.
511	Invalid Pid XML	Invalid PID XML format			Non-compliance with supported Authentication API version structure in CIDR.
512	Invalid Aadhaar holder consent in "rc" attribute of "Auth".	Invalid Aadhaar holder consent in "rc" attribute of "Auth".			
520	Invalid Device	Invalid device			Using any other value other than "public" (all lower case, no spaces or special char) will result in this error.
521	Invalid Finger Device	Invalid Finger device (fdc in Meta element)			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	Invalid Iris device (idc in Meta element)			IDC codes are assigned as part of certification and application developer should use proper idc code given by the iris sensor/extractor vendor
524	Invalid "mi" code under Meta tag				
527	Invalid "mc" code under Meta tag				
530	Invalid AUA Code	Invalid authenticator code			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 AuthXML Version	Invalid Auth XML version			API version used in Auth XML (Authentication request) is either not supported or invalid.
541	Invalid PidXML Version	Invalid PID XML version			Version of the "Pid" element used In the PID XML (Authentication request) is either not supported or invalid.
542	ASA Unauthorized AUA	AUA not authorized for ASA.			This error will be returned if AUA and ASA do not have linking in the portal
543	SubAUA AUA UnAssociated	Sub-AUA not associated with "AUA"			This error will be returned if Sub-AUA specified in "sa" attribute is not added as "Sub-AUA" in portal
550	Invalid Uses Attributes	Invalid "Uses" element attributes			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.
551	Invalid "tid" value	Invalid "tid" value			
553	Registered devices currently not supported. This feature is being implemented in a phased manner.	Registered devices currently not supported. This feature is being implemented in a phased manner.			
554	Public devices are not allowed to be used	Public devices are not allowed to be used			
555	rdsId is invalid and not part of certification registry	rdsId is invalid and not part of certification registry			
556	rdsVer is invalid and not part of certification registry	rdsVer is invalid and not part of certification registry			
557	dpId is invalid and not part of certification registry	dpId is invalid and not part of certification registry			
558	Invalid dih	Invalid dih			
559	Device Certificat has expired	Device Certificat has expired			
560	DP Master Certificate has expired	DP Master Certificate has expired			
561	Expired Pid Request	Request expired ("Pid->ts" value is older than N hours where N is a configured threshold in authentication server)			Either Device/Client/Server date/time is behind current one or old stored pid is getting sent.

562	Future Timestamp Value	Timestamp value is future time (value specified "Pid->ts" is ahead of authentication server time beyond acceptable threshold)			Device/Client/server date/time is ahead than current date/time.
563	Duplicate Auth Request	Duplicate request (this error occurs when exactly same authentication request was re-sent by AUA)			If same "Auth XML" is sent more than once to server, then, 2 nd and subsequent requests will fail with this error.
564	HMAC Validation Failed	HMAC Validation failed			HMAC is not calculated using API defined algorithm
565	License Key Expired	License key has expired			Current License has expired.
566	Invalid License Key	Invalid license key			License key used in application is invalid.
567	Invalid Language Character	Invalid input (this error occurs when some unsupported characters were found in Indian language values, "lname" or "lav")			some unsupported characters were found in Indian language values, "lname" or "lav" in Auth request XML
568	Unsupported Language	Unsupported Language			Value of "lang" attribute is not from the list supported by authapi.
569	Unverified Digital signature	Digital signature verification failed (this means that authentication request XML was modified after it was signed)			Authentication request XML was modified after it was signed.
570	Invalid Digital Certificate	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)			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	PIN Requires reset (this error will be returned if resident is using the default PIN which needs to be reset before usage)			This error will be returned if resident is using the default PIN which needs to be reset before usage.

572	Invalid Biometric Position	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.)			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 Disallowed	Pi usage not allowed as per license			Pi usage not allowed as per license
574	Pa Usage Disallowed	Pa usage not allowed as per license			Pa usage not allowed as per license
575	Pfa Usage Disallowed	Pfa usage not allowed as per license			Pfa usage not allowed as per license
576	FMR Usage Disallowed	FMR usage not allowed as per license			FMR usage not allowed as per license
577	FIR Usage Disallowed	FIR usage not allowed as per license			FIR usage not allowed as per license
578	IIR Usage Disallowed	IIR usage not allowed as per license			IIR usage not allowed as per license
579	OTP Usage Disallowed	OTP usage not allowed as per license			OTP usage not allowed as per license
580	PIN Usage Disallowed	PIN usage not allowed as per license			PIN usage not allowed as per license
581	FuzzyMatch Usage Disallowed	Fuzzy matching usage not allowed as per license			Fuzzy matching usage not allowed as per license
582	Local Language Disallowed	Local language usage not allowed as per license			Local language usage not allowed as per license
584	Invalid Meta Pincode	Invalid Pin code in Meta element			If pincode value is not one of the valid values in UIDAI system, this error occurs
585	Invalid Meta Geocode	Invalid Geo code in Meta element			If geo code does not have proper format as per spec (decimal representation with precision upto 4 decimal values for lat and long), this error occurs
586	FID usage not allowed as per license. This feature is being implemented in a phased manner.	FID usage not allowed as per license. This feature is being implemented in a phased manner.			
587	Name space not allowed				
588	Registered device not allowed as per license				

590	Public device not allowed as per license				
710	Pi Missing	Missing "Pi" data as specified in "Uses"			Missing "Pi" data as specified in "Uses"
720	Pa Missing	Missing "Pa" data as specified in "Uses"			Missing "Pa" data as specified in "Uses"
721	Pfa Missing	Missing "Pfa" data as specified in "Uses"			Missing "Pfa" data as specified in "Uses"
730	PIN Missing	Missing PIN data as specified in "Uses"			Missing PIN data as specified in "Uses"
740	OTP Missing	Missing OTP data as specified in "Uses"			Missing OTP data as specified in "Uses"
800	Invalid Biometric Data	Invalid biometric data			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	Missing biometric data as specified in "Uses"			Missing biometric data as specified in "Uses"
811	Missing CIDR Biometric	Missing biometric data in CIDR for the given Aadhaar number			
812	Best Finger Detection Required	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.			Resident has not done "Best Finger Detection".
820	Missing bt	Missing or empty value for "bt" attribute in "Uses" element			Missing or empty value for "bt" attribute in "Uses" element
821	Invalid bt	Invalid value in the "bt" attribute of "Uses" element			Invalid value in the "bt" attribute of "Uses" element
822	Invalid value in the "bs" attribute of "Bio" element within "Pid".				

901	Auth Data Absent	No authentication data found in the request (this corresponds to a scenario wherein none of the auth data – Demo, Pv, or Bios – is present)			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	Invalid “dob” value in the “Pi” element (this corresponds to a scenario wherein “dob” attribute is not of the format “YYYY” or “YYYY-MM-DD”, or the age of resident is not in valid range)			“dob” attribute is not of the format “YYYY” or “YYYY-MM-DD”, or the age of resident is not in valid range.
910	Invalid Pi mv	Invalid “mv” value in the “Pi” element			
911	Invalid Pfa mv	Invalid “mv” value in the “Pfa” element			
912	Invalid ms Value	Invalid “ms” value			
913	Both Pa pfa Present	Both “Pa” and “Pfa” are present in the authentication request (Pa and Pfa are mutually exclusive)			Attempt to use Pa and Pfa both in the same request can result in this error.
930 to 939	Technical error that are internal to authentication server				
940	Unauthorized ASA Channel	Unauthorized ASA channel			
941	Unspecified ASA Channel	Unspecified ASA channel			
950	Could not generate and/or send OTP	Could not generate and/or send OTP			Retry after some time
951	Biometric lock related technical error	Technical error			Retry after sometime.
980	Unsupported Option	Unsupported option			Currently this error is not reported. Can be used in future.
995	Aadhaar suspended by competent authority.				
996	Aadhaar Cancelled	Aadhaar Cancelled	A401	Aadhaar cancelled being a duplicate. Resident shall use valid Aadhaar.	Aadhaar is no in authenticable status. **Please see ACTN attribute for actionable by the resident.

			A402	Aadhaar cancelled due to disputed enrolment. Shall re-enrol if resident doesn't have a valid Aadhaar.	
			A403	Aadhaar cancelled due to technical Issues. Resident shall contact UIDAI contact centre.	
			A404	Aadhaar cancelled due to disputed enrolment (BE). Shall re-enrol if resident doesn't have a valid Aadhaar.	
			A405	Aadhaar cancelled due to erroneous enrolment (Iris). Shall re-enrol if resident doesn't have a valid Aadhaar.	
997	Aadhaar Suspended	Aadhaar Suspended	A301	Aadhaar suspended due to inactivity. Resident shall follow the Reactivation process.	Aadhaar is not in Auhenticatable status. **Please see ACTN attribute for actionable by the resident.
			A302	Aadhaar suspended due to Biometrics integrity issue. Resident shall visit Permanent Enrolment Centre with document proofs for update.	
			A303	Aadhaar suspended due to Demographic integrity issue. Resident shall visit Permanent Enrolment Centre / UIDAI website with document proofs for update.	
			A304	Aadhaar suspended due to Address dispute. Resident shall visit Permanent Enrolment Centre with document proofs for update.	

			A305	Aadhaar suspended due to Photo dispute. Resident shall visit Permanent Enrolment Centre with document proofs for update.	
			A306	Aadhaar suspended due to Age dispute. Resident shall update the age.	
			A307	Aadhaar suspended since child has not updated biometrics after age of 5. Resident shall update the biometrics.	
			A308	Aadhaar suspended since resident has not updated biometrics after age of 15. Resident shall update the biometrics.	
			A309	Aadhaar is locked by resident. Resident shall follow the Un-locking process.	
998	Unavailable Aadhaar Number	Invalid Aadhaar Number Or Non Availability of Aadhaar data	A201	Aadhaar number is incorrect. Resident shall use correct Aadhaar.	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	Unknown error	A202	Authentication temporarily not available, resident shall retry after sometime.	
E-000	Bad Request HTTP Received	Https request should be sent		Https request should be sent	
E-001	Bad Request GET Received	Only post request should be sent		Only post request should be sent	

E-100	Unparsable Auth XML	XML format or the attribute values are not proper		XML format or the attribute values are not proper	
E-101	Unparsable KYC XML	XML format or the attribute values are not proper		XML format or the attribute values are not proper	
E-102	Request DB Auditing Failed	Transaction id length exceeds the range specified by UIDAI or db connection issues.		XML format or the attribute values are not proper	
E-103	Response DB Auditing Failed	Improper response or problems in app connection or db connection issues.		Transaction id length exceeds the range specified by UIDAI or db connection issues.	
E-104	Error DB Auditing Failed	Transaction id length exceeds the range specified by UIDAI or db connection issues.		Improper response or problems in app connection or db connection issues.	
E-105	KYC XSD Validation Failed	XML format or the attribute values are not proper		Transaction id length exceeds the range specified by UIDAI or db connection issues.	
E-106	KYC Request Signature Verification Failed	1) Private key used for signing is not correct or public key used for verifying is not correct 2) Data being sent was altered after signing. 3)			XML format or the attribute values are not proper
E-107	Auth Request signature verification failed	1) Private key used for signing is not correct or public key used for verifying is not correct 2) Data being sent was altered after signing. 3) Signing mechanism used is not correct.			1) Private key used for signing is not correct or public key used for verifying is not correct 2) Data being sent was altered after signing. 3) Signing mechanism used is not correct.
E-108	AUA IP Verification Failed at UIDAI	Entity IP address is not mapped to UIDAI		1) Private key used for signing is not correct or public key used for verifying is not correct 2) Data being sent was altered after signing. 3) Signing mechanism used is not correct.	

E-109	Blank UIDAI Response	Connection could not be established with UIDAI		Entity IP address is not mapped to UIDAI	
E-110	KSA Response Decryption Error	Issue while decrypting the response		Connection could not be established with UIDAI	
E-111	KYC Response Signature Verification Failed	Issue at UIDAI end, signature might be missing in the response or public key used is incorrect		Issue while decrypting the response	
E-112	BFD XSD validation failed	XML format or the attribute values are not proper			Issue at UIDAI end, signature might be missing in the response or public key used is incorrect
E-113	OTP XSD validation failed	XML format or the attribute values are not proper		XML format or the attribute values are not proper	
E-114	Unparsable KYC Response XML	XML format or the attribute values are not proper			XML format or the attribute values are not proper
E-115	Unparsable Auth Response XML	XML format or the attribute values are not proper			XML format or the attribute values are not proper
E-116	Signed Auth XML Generation Error	Certificate			XML format or the attribute values are not proper
E-117	Signed KYC XML Generation Error	Certificate			Certificate Missing/incorrect logic for signed xml generation
E-118	Auth response signature verification failed	Issue at UIDAI end, signature might be missing in the response or public key used is incorrect			Certificate Missing/incorrect logic for signed xml generation
E-119	ASA-UIDAI Connection Error	Connection issue at			Issue at UIDAI end, signature might be missing in the response or public key used is incorrect
E-120	Auth XSD validation failed	XML format or the attribute values are not proper			Connection issue at UIDAI end/NSDL end.
E-122	Property file unavailable	Check property file available at respective locations.			XML format or the attribute values are not proper
E-123	Unparsable BFD Request XML	XML format or the attribute values are not proper			Check property file available at respective locations.
E-124	Unparsable OTP Request XML	XML format or the attribute values are not proper			XML format or the attribute values are not proper

E-125	BFD request signature verification failed	1) Private key used for signing is not correct 2) Data being sent was altered after signing. 3) Signing mechanism used is not correct.			1) Private key used for signing is not correct 2) Data being sent was altered after signing. 3) Signing mechanism used is not correct.
E-126	OTP request signature verification failed	1) Private key used for signing is not correct 2) Data being sent was altered after signing. 3)		1) Private key used for signing is not correct 2) Data being sent was altered after signing. 3) Signing mechanism used is not correct.	
E-127	Signed BFD XML	Certificate		Certificate Missing/incorrect logic for signed xml generation	
E-128	Signed OTP XML	Certificate		Certificate Missing/incorrect logic for signed xml generation	
E-129	Unparsable BFD Response XML	Issue at UIDAI end		Issue at UIDAI end	
E-130	Unparsable OTP Response XML	Issue at UIDAI end		Issue at UIDAI end	
E-131	XML Decryption Certificate Error	Certificate might not have rights of decryption		Certificate might not have rights of decryption	
E-132	KYC Request Signature Verification Error	Signature is missing in request XML or public key file is missing		Signature is missing in request XML or public key file is missing	
E-133	KYC Response Signature Verification Error	Issue at UIDAI end, signature might be missing in response XML or public key file is missing		Issue at UIDAI end, signature might be missing in response XML or public key file is missing	
E-134	Auth Request Signature Verification Error	Signature is missing in XML or public key file is missing		Signature is missing in XML or public key file is missing	
E-135	Auth Response Signature Verification Error	Signature is missing in XML or public key file is missing		Signature is missing in XML or public key file is missing	
E-136	BFD Request Signature Verification Error	Signature is missing in XML or public key file is missing		Signature is missing in XML or public key file is missing	

E-137	OTP Request Signature Verification Error	Issue at UIDAI end, signature might be missing in response XML or public key file is missing		Issue at UIDAI end, signature might be missing in response XML or public key file is missing	
E-138	KYC XSD Validation Error	XSD file is missing,Check if XSD file is present		XSD file is missing,Check if XSD file is present	
E-139	Auth XSD Validation Error	XSD file is missing,Check if XSD file is present		XSD file is missing,Check if XSD file is present	
E-140	BFD XSD Validation Error	XSD file is missing,Check if XSD file is present		XSD file is missing,Check if XSD file is present	
E-141	OTP XSD Validation Error	XSD file is missing,Check if XSD file is present		XSD file is missing,Check if XSD file is present	
E-142	AUA IP Verification Failed at NSDL	Entity not mapped in database for respective subaua code.		Entity not mapped in database for respective subaua code.	
E-143	E Response Received	Problem in the application		Problem in the application	
E-144	BFD Response Signature Verification Failed	Issue at UIDAI end, signature might be missing in response XML or public key file is missing		Issue at UIDAI end, signature might be missing in response XML or public key file is missing	
E-145	OTP Signature Tag Missing in Request XML	Refer to the standard of without sign OTP request.	Signature tag is missing in OTP request XML		
E-199	KSA/ASA Internal Error	Problem in the application		Problem in the application	
E-200	Mandatory Sub-Aua Null Element	One of the mandatory		One of the mandatory Sub Aua elements is null.	
E-201	strSaCd Parameter Validation Error	strSaCd(Sub AUA Code) parameter is missing or value is not correct		strSaCd(Sub AUA Code) parameter is missing or value is not correct	
E-203	strAadhaar Parameter Validation Error	strAadhaar(Aadhaar No.) parameter is missing or value is not correct		strAadhaar(Aadhaar No.) parameter is missing or value is not correct	
E-204	strAadhaarName Parameter Validation Error	strAadhaarName(Aadhaar Card Holder name) parameter is missing or		strAadhaarName(Aadhaar Card Holder name) parameter is missing or value is not correct	
E-205	strYear Parameter Validation Error	strYear parameter is missing or value is not correct		strYear parameter is missing or value is not correct	

E-206	strGender Parameter Validation Error	strGender parameter is missing or value is not correct		strGender parameter is missing or value is not correct	
E-207	trTransId Parameter Validation Error	strTransId parameter is missing or value is not correct		strTransId parameter is missing or value is not correct	
E-208	strUDC Parameter Validation Error	strUDC parameter is missing or value is not correct		strUDC parameter is missing or value is not correct	
E-209	strMV Parameter Validation Error	strMV parameter is missing or value is not correct		strMV parameter is missing or value is not correct	
E-210	mvThreshold Value not in range 1-100	Value of mvThreshold is not within the range		Value of mvThreshold is not within the range	
E-211	strLang Parameter Validation Error	strLname is present but strLang is missing		strLname is present but strLang is missing	
E-212	strLmv Value not in range 1-100	Value of parameter strLmv is not in the range		Value of parameter strLmv is not in the range	
E-213	Signing Certificate Verification Failed	Signature element forwarded is not proper		Signature element forwarded is not proper	
E-214	strOtp Parameter Validation Error	strOtp parameter is missing or value is not correct		strOtp parameter is missing or value is not correct	
E-215	strRequestType Parameter Validation Error	strRequestType parameter is missing or value is not correct		strRequestType parameter is missing or value is not correct	
E-216	strBioType Parameter Validation Error	strBioType parameter is missing or value is not correct		strBioType parameter is missing or value is not correct	
E-217	strFingerOnePos Parameter Validation Error	strFingerOnePos parameter is missing or value is not correct		strFingerOnePos parameter is missing or value is not correct	
E-218	strFingerTwoPos Parameter Validation Error	strFingerTwoPos parameter is missing or value is not correct		strFingerTwoPos parameter is missing or value is not correct	
E-219	strMS Parameter Validation Error	strMS parameter is missing or value is not correct		strMS parameter is missing or value is not correct	

E-220	Blank Signature Tag Exception	Please make sure that AUA/KUA Code is present in the Signature Tag for IP Verification for ASA/KSA Signing	Signature Tag parameter length is 0		
E-221	Incorrect OTP Version	Please make sure that the OTP Version is 1.6 for generating verification code	OTP Version is Incorrect		
E-222	Error during MOU Request Signature Verification	Please check for the signature. If signature is there, but still getting error then forward the same to NSDL team for further action	Signature is missing in request XML or public key file is missing		
E-223	Error during MOU Response Signature Verification	Forward the same to NSDL team	Issue at UIDAI end, signature might be missing in response XML or public key file is missing		
E-224	Error during MOU XSD Validation	Forward the same to NSDL team	XSD file is missing, Check if XSD file is present		
E-225	MOU XSD Validation Failed	Refer to the standard MOU XML format and check all the attributes and their value	XML format or the attribute values are not proper		
E-226	MOU Request Signature Verification Failed	Please ensure that private key and mechanism used for signing is correct. Also, ensure that data is not changed after signing	1) Private key used for signing is not correct or public key used for verifying is not correct 2) Data being sent was altered after signing. 3) Signing mechanism used is not correct.		

E-227	MOU Response Signature Verification Failed	Forward the same to NSDL team to further check it with UIDAI	Issue at UIDAI end, signature might be missing in the response or public key used is incorrect		
E-228	MOU XML Not Parsed Properly	Refer to the standard MOU XML format and check all the attributes and their value. If everything seems to be correct, then contact nsdl team for further action.	XML format or the attribute values are not proper		
E-229	MOU Response XML Not Parsed Properly	Refer to the standard MOU XML format and check all the attributes and their value. If everything seems to be correct, then contact nsdl team for further action.	XML format or the attribute values are not proper		
E-230	Signing Certificate Verification Error	Check the form signer components		Check the form signer components	
E-231	Signed MOU XML Generation Error	Report the same to NSDL team for further action	Certificate Missing/incorrect logic for signed xml generation		
E-232	RESIDENT AUTH XML Not Parsed Properly	Refer to the standard Auth XML format and check all the attributes and their value. If everything seems to be correct, then contact nsdl team for further action.	XML format or the attribute values are not proper		
E-233	OPERATOR AUTH XML Not Parsed Properly	Refer to the standard Auth XML format and check all the attributes and their value. If everything seems to be correct, then contact nsdl team for further action.	XML format or the attribute values are not proper		
E-234	MOU Signature Tag Missing in Request XML	Refer to the standard of without sign MUA request.	Signature tag is missing in MOU request XML		

E-235	Request Signature Verification Failed	Please ensure that private key and mechanism used for signing is correct. Also check if proper certificate is mapped on the Server.	1) Private key used for signing is not correct or public key used for verifying is not correct 2) Signing mechanism used is not correct.		
E-236	Error during Request Signature Verification	Please check for the signature. If error exists then check if public certificate is present on the server or if data is getting altered after signing else forward the same to NSDL team for further action	Public key file is missing or data is getting altered after signing		
E-237	Error during KYC Response Encryption	Please check with NSDL e-Gov.	Encryption public key is not mapped at NSDL		
E-300	Some server error while processing the request	Some server error while processing the request			
E-301	Invalid API Version	Invalid API Version			
E-302	Invalid Client Details	Invalid Client Details			
E-303	Client Licence key expire	Client Licence key expire			
E-304	Request XML not available.	Request XML not available.			
E-307	Failed to connect UIDAI Server! Please try after some time	Failed to connect UIDAI Server! Please try after some time			
E-308	Failed to parse Response XML	Failed to parse Response XML			
E-555	Duplicate transaction id error	Transaction id is duplicate		Transaction id is duplicate	
E-563	UIDAI Connection Read Timeout	Connectivity issue with UIDAI		Connectivity issue with UIDAI	
E-999	KSA Internal Error	KSA Internal Error			
K-100	Resident Authentication Failed	Resident authentication failed			
K-200	Resident Data Unavailable	Resident data currently not available			
K-540	Invalid KYC XML	Invalid KYC XML			
K-541	KYC API Invalid	Invalid KYC API version			
K-542	Invalid rc Attribute	Invalid resident consent			
K-543	Invalid ts Attribute	Invalid timestamp			
K-544	Invalid ra Attribute	Invalid resident auth type			
K-545	Resident Opted Out	Resident has opted out of this service			

K-546	Invalid value for pfr attribute	KYC 2.0 error code. Invalid value for pfr attribute.			
K-547	Invalid value for "wadh" attribute within PID block				
K-550	Invalid Uses Element	Invalid Uses attribute			
K-551	Invalid "Txn" namespace	Invalid "Txn" namespace			
K-552	Invalid License Key	Invalid license key			
K-569	Unverified Digital Signature	Digital signature verification failed for KYC XML (means that authentication request XML was modified after it was signed)			
K-570	Invalid Digital Certificate	Invalid key info in digital signature for KYC XML (it is either expired, or does			
K-600	Unauthorized KUA	AUA is invalid or not an authorized KUA			
K-601	Unauthorized KSA	ASA is invalid or not an authorized KSA			
K-602	KUA Encryption Key Unavailable	KUA encryption key not available			
K-603	KSA Encryption Key Unavailable	KSA encryption key not available			
K-604	KSA disallowed Signing	KSA not allowed to sign			
K-605	Neither KUA key nor KSA encryption key are available	KYC 2.0 error code. Neither KUA key nor KSA encryption key are available			
K-955	Technical Error	Technical error			
K-999	Unknown Error	Unknown Error			

SRDH ERROR CODES

Error Codes	Description	Probable Reason
800	Internal Server Error	Technical Reason. User Suggested to try again.
801	Error in creating AUA service Request	Error in creating AUA service Request
802	Error in parsing AUA request XML	Error in creating AUA service Request
803	Error in parsing AUA response xml	Error in parsing AUA request XML
804	Invalid Sub AUA/ License Key	Error in parsing AUA response xml
805	Sub AUA license expired	Sub AUA license expired
806	Domain ID not present	Domain ID not present
807	Invalid Aadhaar ID	Invalid Aadhaar ID
808	Invalid name (In case the name field contains any special characters or numbers in it this error code will returned by SRDH. Valid name will be as registered with UIDAI)	Invalid name
809	Invalid email (Valid email id example: abc@test.com)	Invalid email
810	Invalid Phone (Phone number should contain exactly 10 digits)	Invalid Phone
811	Missing input (In case of any of the mentioned attribute is missing SRDH will generate this error code)	Required input is missing.
812	In case of demographic authentication one should provide either name, phone or email along with uid field otherwise this error code will be generated by SRDH	Required input is missing.
813	Biometric Input is Missing	Biometric Input is Missing
814	Duplicate Transaction ID	Duplicate Transaction ID
815	Invalid transaction ID	Invalid Transaction ID
816	Invalid UDC	Incorrect UDC specified.
817	Error in creating OTP service request	Technical Reason. User Suggested to try again.
818	Missing OTP input	Missing OTP input
819	Invalid uses flag values	Uses flag values are not correct. User suggested to check for the same
820	Missing "langCode" input	Missing "langCode" input
821	Invalid domain ID length	Domain ID with length greater than 50 char is passed in domainId attribute
827	System Admin Error	System Admin Error
828	Pin Request is not yet Supported by UIDAI	Unsupported PIN Request
829	Department Code Not Present	Department code is not present
830	Invalid Department Code	Department code is not correct
831	Invalid TimeStamp Value	Time stamp is not correct
832	Invalid Iris Type	Invalid Iris Type
833	Invalid Iris Count	Invalid Iris Count
834	Invalid Finger Record Type	Invalid Finger Record Type
835	Invalid Finger Record Count	Invalid Finger Record Count

836	Invalid Terminal Id	Invalid Terminal Id
837	Invalid txn value	Invalid txn value for OTP eKYC
851	Missing input (In case of any of the mentioned attribute is missing SRDH will generate this error code)	Required input is missing.
901	Error in creating KUA service Request	Technical Error. User is suggested to try again.
902	Error in parsing KUA request XML	Technical Error. User is suggested to try again.
903	Error in parsing KUA response xml	Technical Error. User is suggested to try again.
904	Consent value has not set or it is set to 'n'	Consent not captured. Suggested to retry after taking resident's consent
905	Invalid IData value	KYC 2.0 SRDH error code. Invalid IData value
906	Invalid MEC value	KYC 2.0 SRDH error code. Invalid MEC value
907	Invalid DE value	KYC 2.0 SRDH error code. Invalid DE value
908	Invalid PFR value	KYC 2.0 SRDH error code. Invalid PFR value
910	Invalid RA value	KYC 2.1 SRDH error code. Invalid RA value
M-301	Request XML not Received at SRDH. Please Try Again.	Technical Error. User Suggested to try again.
M-302	XSD Validation Failed at SRDH. Please Try Again.	Technical Error. User Suggested to try again.
M-303	Mandatory Sub-Aua Null Element at SRDH	Technical Error. User Suggested to try again.
M-304	Mandatory Sub-Aua Blank Element at SRDH	Technical Error. User Suggested to try again.
M-305	Invalid sa Parameter Received at SRDH	Technical Error. User Suggested to try again.
M-306	ASA Connection Read Timeout. Please Try Again.	Technical Error. User Suggested to try again.
M-307	Unparsable Auth Request XML at SRDH. Please Try Again.	Technical Error. User Suggested to try again.
M-308	No Signature in Request XML Received at SRDH. Please Try Again.	Technical Error. User Suggested to try again.
M-309	Improper Response Received from ASA. Please Try Again.	Technical Error. User Suggested to try again.
M-310	Unparsable Auth Response at SRDH. Please Try Again.	Technical Error. User Suggested to try again.
M-311	Unverified Signature in Request XML Received at SRDH. Please Try Again.	Technical Error. User Suggested to try again.
M-333	SRDH Internal Error. Please Try Again.	Technical Error. User Suggested to try again.