SHREETRON INDIA LIMITED

AUA-KUA 2.5 API DOCUMNET

Version-2.5.0.1.0.1

INDEX

1. OTP Generation

Requesting to WEB API to generate OTP

Request

Method	URL
POST	<webapi-url>/auakua/pre/api/AuaKuaClientGateway/otp

XML format for OTP Generation

<SynOtp lat="" lon="" devmacid="" devid="" rc="" shrc="" ver="" sertype="" env="" ch="" udc="" uid="" slk="" rrn="" ref="">
</SynOtp>

Element Details

<SynOtp>

- Mandatory Root element of the input XML for OTP generation service.

Request Attributes

Attribute	Type	Description
lat	string	Latitude
long	String	Longitude
devmacid	string	Device MacID
devid	string	Device ID
rc	string	Resident consent(Y)
shrc	string	Shared Resident consent(Y)
ver	string	version of the API. Currently only valid value is "2.5".
sertype	string	Based on Service type, the value to be passed is as mentioned below. Auth OTP Gen - 09

		eKyc OTP Gen - 10
env	string	Environment value 2- for API
ch	string	Channel through which OTP should be sent. Possible values are: • "0" – send OTP via both SMS and Email (this is the default) • "1" – send OTP via SMS only • "2" – send OTP via Email only
udc	String	Unique Host Device Code. This is an alpha-numeric string of maximum length 20.
uid	string	Aadhaar Number/Virtual ID/UID Token. (if you don't want to pass uid pass empty) Aadhaar Number=12 digits Virtual ID=16 digits UID Token=72 digits(Alpha Numeric)
slk	string	License Key given by Shreetron
rrn	string	Your request transaction ID (Max 50 in length)
ref	string	Any Client Reference Data (Max 50 length)

Response

```
{
 "ret": "y",
 "code": "XXXXXXXXXXXXXXXXX",
 "txn": "XXXXXXXXXXXXXXXXX",
 "ts": "XXXXXXXXXXXXXXXXX",
 "err": "000",
 "errdesc": "",
 "rrn": "XXXXXXXXXXXXXXXXX",
 "ref":"client-ref-data",
 "responseXml": "Base64 response string"
 }
```

Response Attributes

Attribute	Type	Description
ret	string	Result of OTP generation request. “y” if successful, “n” if failure
code	String	Unique alphanumeric “OTP response” code having maximum length 40.
txn	string	AUA specific transaction identifier.
ts	string	Timestamp when the response is generated
err	string	Failure error code
errdesc	string	Failure error description
rrn	string	Your request transaction ID
ref	string	Your Reference Data Sent in Request
responseXML	String	OTP Response in Base64 Encoded XML format. Refer **Annexure B** for the format.

2. Authentication with OTP

Requesting to WEB API to authenticate using generated OTP.

Request

Method	URL
POST	<webapi-url>/auakuapre/api/AuaKuaClientGateway/auth

Following is the XML data format for OTP API

```
<SynAuth lat="" lon="" devmacid="" devid="" rc="" shrc="" ver="" udc="" otp="" sertype="" env="" uid="" txn="" slk="" rrn="" ref="" >
<Skey ci=""> encrypted and encoded session key</Skey>
<Data type="X"> encrypted PID block</Data>
<Hmac> SHA-256 Hash of Pid block, encrypted and then encoded</Hmac>
</SynAuth>
```

Element Details

Element: **SynAuth** (mandatory)

- Root element of the input XML for authentication service.

Request Attributes

Attribute	Type	Description
lat	string	Latitude
long	string	Longitude
devmacid	string	Device MAcID
devid	string	Device ID
rc	string	Resident consent(Y)
shrc	string	Sharing Consent(Y)
ver	string	version of the API. Currently only valid value is "2.5".
udc	string	Unique Host Device Code. This is an alpha-numeric string of maximum length 20.
otp	string	OTP value
sertype	string	Based on Service type, the value to be passed is as mentioned below. Auth with OTP-02
env	string	Environment value 2- for API
uid	string	Aadhaar Number/Virtual ID/UID Token. (if you don't want to pass uid pass empty) Aadhaar Number=12 digits Virtual ID=16 digits UID Token=72 digits(Alpha Numeric)
txn	string	Txn value should be pass in the response of OTP generation
slk	string	License Key generated by Shreetron

rrn	string	Your request transaction ID (Max 50 in length)
ref	string	Any Client Reference Data (Max 50 length)
dc	string	
rdsId	string	
rdsVer	string	
dpId	string	
udc	string	Unique Host Device Code. This is an alpha-numeric string of maximum length 20.
mi	string	
mc	string	
Skey	string	
ci	string	
Data	string	
type	string	
Hmac	string	

Response

```
{
 "ret": "y",
 "code": "XXXXXXXXXXXXXXXXX",
 "txn": "XXXXXXXXXXXXXXXXX",
 "ts": "XXXXXXXXXXXXXXXXX",
 "err": "000",
 "errdesc": "",
 "rrn": "XXXXXXXXXXXXXXXXX"
 “ref”:”client-ref-data”,
 "responseXML": "Base64 response string",
}
```

Response Attributes

Attribute	Type	Description
ret	string	Result of OTP generation request. “y” if successful, “n” if failure
code	String	Unique alphanumeric “OTP response” code having maximum length 40.
txn	string	AUA specific transaction identifier.
ts	string	Timestamp when the response is generated
err	string	Failure error code
errdesc	string	Failure error description
rrn	string	Your request transaction ID
ref	string	Your Reference Data Sent in Request
responseXML	String	Authentication Response in Base64 Encoded XML format. Refer **Annexure B** for the format.

3. Authentication with BIOMETRIC / IRIS

Requesting to WEB API to authenticate using Biometric.

Request

Method	URL
POST	<webapi-url>/auakuapre/api/AuaKuaClientGateway/auth

Following is the XML data format for authentication API

```
<SynAuth lat="" lon="" devmacid="" devid="" devsrno="" rc="" shrc="" ver="" sertype="" env="" uid="" slk="" rrn="" ref="">
<Meta dc="" rdsId="" rdsVer="" dpId="" udc="" mi="" mc="" />
<Skey ci=""> encrypted and encoded session key</Skey>
<Data type="X"> encrypted PID block</Data>
<Hmac> SHA-256 Hash of Pid block, encrypted and then encoded</Hmac>
</SynAuth>
```

Element Details

Element: **SynAuth** (mandatory)

- Root element of the input XML for authentication service.

Request Attributes

Attribute	Type	Description
lat	string	Latitude
long	string	Longitude
devmacid	string	Device MAcID
devid	string	Device ID
devsrno	string	Device Serial Number
rc	string	Resident Consent(Y)
shrc	string	Shared Consent(Y)
ver	string	version of the Auth API. Currently only valid value is “2.5”.
sertype	string	Based on Service type, the value to be passed is as mentioned below. Auth with Bio – 01 Auth with IRIS - 03
env	string	Environment value 2- for API
uid	string	Aadhaar Number/Virtual ID/UID Token. (if you don’t want to pass uid pass empty) Aadhaar Number=12 digits Virtual ID=16 digits UID Token=72 digits(Alpha Numeric)
slk	string	License Key given by Shreetron
rrn	string	Your request transaction ID (Max 50 in length)

ref	string	Any Client Reference Data (Max 50 length)
dc	string	
rdsId	string	
rdsVer	string	
dpId	string	
udc	string	Unique Host Device Code. This is an alpha-numeric string of maximum length 20.
mi	string	
mc	string	
Skey	string	
ci	string	
Data	string	
type	string	
Hmac	string	

Response

```
{
 "ret": "y",
 "code": "XXXXXXXXXXXXXXXXX",
 "txn": "XXXXXXXXXXXXXXXXX",
 "ts": "XXXXXXXXXXXXXXXXX",
 "err": "000",
 "errdesc": "",
 "rrn": "XXXXXXXXXXXXXXXXX",
 “ref”:”client-ref-data”,
 "responseXML": "Base64 response string"
}
```

Response Attributes

Attribute	Type	Description

ret	string	Result of OTP generation request. “y” if successful, “n” if failure
code	String	Unique alphanumeric “OTP response” code having maximum length 40.
txn	string	AUA specific transaction identifier.
ts	string	Timestamp when the response is generated
err	string	Failure error code, in case of success it is 000.
errdesc	string	Failure error description
rrn	string	Your request transaction ID
ref	string	Your Reference Data Sent in Request
responseXML	String	Authentication Response in Base64 Encoded XML format. Refer **Annexure B** for the format.

4. Authentication with Demographic

Requesting to WEB API to authenticate using Demographic Data.

Request

Method	URL
POST	<webapi-url>/auakuapre/api/AuaKuaClientGateway/auth

Following is the XML data format for authentication API

```
<SynAuth lat="" lon="" devmacid="" devid="" devsrno="" rc="" shrc="" ver="" sertype="" env="" uid="" slk="" rrn="" ref="" udc="" pi="" pa="" pfa=""><Skey ci=""></Skey>
<Data type="X"></Data>
<Hmac></Hmac>
</SynAuth>
```

Element Details

Element: **SynAuth** (mandatory)

- Root element of the input XML for authentication service.

Request Attributes

Attribute	Type	Description
lat	string	Latitude
long	string	Longitude
devmacid	string	Device MAcID
devid	string	Device ID
devsrno	string	Device Serial Number
rc	string	Resident Consent(Y)
shrc	string	Shared Consent(Y)
ver	string	version of the Auth API. Currently only valid value is “2.5”.
sertype	string	Based on Service type, the value to be passed is as mentioned below. Auth with Demographic – 07
env	string	Environment value 2- for API
uid	string	Aadhaar Number/Virtual ID/UID Token. (if you don’t want to pass uid pass empty) Aadhaar Number=12 digits Virtual ID=16 digits UID Token=72 digits(Alpha Numeric)
slk	string	License Key given by Shreetron
rrn	string	Your request transaction ID (Max 50 in length)
ref	string	Any Client Reference Data (Max 50 length)

pi	string	Valid values are “y” or “n”. If the value is “y” then at least one attribute of element “Pi” (part of “Demo” element) should be used in authentication. If value is “n”, “Pi” element is not mandated.
pa	string	Valid values are “y” or “n”. If the value is “y” then at least one attribute of element “Pa” (part of “Demo” element) should be used in authentication. If value is “n", “Pa” element is not mandated.
pfa	string	Valid values are “y” or “n”. If the value is “y” then element “Pfa” (part of “Demo” element) should be used in authentication. If value is “n”, “Pfa” element is not mandated.
udc	string	Unique Host Device Code. This is an alpha-numeric string of maximum length 20.
Skey	string	Value of this element is base-64 encoded value of encrypted 256-bit AES session key.
ci	string	Public key certificate identifier
Data	string	Contains the encrypted “Pid” element in base-64 format.
type	string	Type of the PID block format. It can have tw values – “X” for XML and “P” for Protobuf binary format. Default value is assumed to “X”.
Hmac	string	After forming Pid XML, compute SHA-256 hash of Pid XML string and encrypt using session key then it should be base 64 encoded.

Response

```
{
 "ret": "y",
 "code": "XXXXXXXXXXXXXXXXX",
```

```
"txn": "XXXXXXXXXXXXXXXXX",
"ts": "XXXXXXXXXXXXXXXXX",
"err": "000",
"errdesc": "",
"rrn": "XXXXXXXXXXXXXXXXX",
“ref”:”client-ref-data”,
"responseXML": "Base64 response string"
}
```


Response Attributes

Attribute	Type	Description
ret	string	Result of OTP generation request. “y” if successful, “n” if failure
code	String	Unique alphanumeric “OTP response” code having maximum length 40.
txn	string	AUA specific transaction identifier.
ts	string	Timestamp when the response is generated
err	string	Failure error code, in case of success it is 000.
errdesc	string	Failure error description
rrn	string	Your request transaction ID
ref	string	Your Reference Data Sent in Request
responseXML	String	Authentication Response in Base64 Encoded XML format. Refer **Annexure B** for the format.

5. E-KYC with OTP

Requesting to WEB API to authenticate using OTP

Request

Method	URL
POST	<webapi-url>/auakuapre/api/AuaKuaClientGateway/kyc

Following is the XML data format for authentication API

<SynKyc lat="" lon="" devmacid="" devid="" rc="" shrc="" lr="" pfr="" ver="" sertype="" env="" uid="" udc="" otp="" txn="" slk="" rrn="" ref="" >
<Skey ci="">encrypted and encoded session key</Skey>
<Data type="X">encrypted PID block</Data>
<Hmac>SHA-256 Hash of Pid block, encrypted and then encoded</Hmac>
</SynKyc>

Element Details

Element: **SynKyc** (mandatory)

- Root element of the input XML for e-KYC API.

Request Attributes

Attribute	Type	Description
lat	int	Latitude
long	string	Longitude
devmacid	string	Device MacID
devid	string	Device ID
rc	string	Resident Consent(Y)
shrc	string	Shared Consent(Y)
lr	string	AUA application require local language data in addition to English (N)
pfr	string	Print format request flag for retrieving E-Aadhaar document in PDF (N)
ver	string	version of the KYC API. Currently only valid value is “2.5”.
sertype	string	Based on Service type, the value to be passed is as mentioned below. Kyc with OTP - 05

env	string	Environment value 2- for API
uid	string	Aadhaar Number/Virtual ID/UID Token. (if you don't want to pass uid pass empty) Aadhaar Number=12 digits Virtual ID=16 digits UID Token=72 digits(Alpha Numeric)
udc	string	Unique Host Device Code. This is an alpha-numeric string of maximum length 20.
otp	string	OTP value
txn	string	Txn value should be pass in the response of OTP generation
slk	string	License Key given by shreetron
rrn	string	Your request transaction ID (Max 50 in length)
ref	string	Any Client Reference Data (Max 50 length)
dc	string	
rdsId	string	
rdsVer	string	
dpId	string	
udc	string	Unique Host Device Code. This is an alpha-numeric string of maximum length 20.
mi	string	
mc	string	
Skey	string	
ci	string	
Data	string	

type	string	
Hmac	string	

e-KYC API: Response Data Format

Resident data as part of the response based on successful authentication (thus resident authorizing UDIAI to share his/her data with the KUA/ASA) is in base 64 encoded format.

Response

```
{
 "ret": "y",
 "code":"XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
 "txn": "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
 "ts": "XXXXXXXXXXXXXXXXXXXXX",
 "err": "000",
 "errdesc": "",
 "rrn": "XXXXXXXXXXXXX",
 “ref”:”client-ref-data”,
 "responseXML": "Base64 encoded string"
}
```

Failure Response

```
{
 "ret": "n",
 "code": "XXXXXXXXXXXXXXXXXXXXXXXXxxxx",
 "txn":   "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
 "ts": "XXXXXXXXXXXXXXXXXXXXX",
 "err": "XXXXXXXXX",
 "errdesc":"XXXXXXXXXXXXX",
 "rrn": "XXXXXXXXXXXXX",
 “ref”:”client-ref-data”,
 "responseXML": “Base64 encoded string"
}
```

Response Attributes

Attribute	Type	Description
ret	string	Result of OTP generation request. “y” if successful, “n” if failure
code	String	Unique alphanumeric “OTP response”

		code having maximum length 40.
txn	string	AUA specific transaction identifier.
ts	string	Timestamp when the response is generated
err	string	Failure error code, in case of success it is 000.
errdesc	string	Failure error description
rrn	string	Your request transaction ID
ref	string	Your Reference Data Sent in Request
responseXML	String	E-Kyc Response in Base64 Encoded XML format. Refer **Annexure B** for the format.

6. E-KYC with BIOMETRIC / IRIS

Requesting to WEB API to authenticate using Biometric / IRIS.

Request

Method	URL
POST	<webapi-url>/auakuapre/api/AuaKuaClientGateway/kyc

Following is the XML data format for authentication API

```
<SynKyc lat="" lon="" devmacid="" devid="" devsrno="" rc="" shrc="" lr="" pfr="
 "ver="" sertype="" env="" uid="" slk="" rrn="" ref="" >
<Meta udc=" " dpId=" " rdsId=" " rdsVer=" " mi=" " mc=" "/>
<Skey ci=" "> encrypted and encoded session key </Skey>
<Data type="X"> encrypted PID block </Data>
<Hmac> SHA-256 Hash of Pid block, encrypted and then encoded </Hmac>
</SynKyc>
```

Element Details

Element: **SynKyc** (mandatory)

- Root element of the input XML for e-KYC API.

Request Attributes

Attribute	Type	Description
lat	int	Latittude
long	string	Longitude
devmacid	string	Device MAcID
devid	string	Device ID
rc	string	Resident Consent(Y)
shrc	string	Shared Consent(Y)
lr	string	AUA application require local language data in addition to English (N)
pfr	string	Print format request flag for retrieving E-Aadhaar document in PDF (N)
ver	string	Kyc Version (2.5 for RD)
sertype	string	Based on Service type, the value to be passed is as mentioned below. Kyc with Bio – 04 Kyc with Iris - 06
env	string	Environment value 2- for API
uid	string	Aadhaar Number/Virtual ID/UID Token. (if you don't want to pass uid pass empty) Aadhaar Number=12 digits Virtual ID=16 digits UID Token=72 digits(Alpha Numeric)
slk	string	License key given by shreetron
rrn	string	Your request transaction ID (Max 50 in length)

ref	string	Any Client Reference Data (Max 50 length)
dc	string	
rdsId	string	
rdsVer	string	
dpId	string	
udc	string	Unique Host Device Code. This is an alpha-numeric string of maximum length 20.
mi	string	
mc	string	
Skey	string	
ci	string	
Data	string	
type	string	
Hmac	string	

e-KYC API: Response Data Format

Resident data as part of the response based on successful authentication (thus resident authorizing UDIAI to share his/her data with the KUA/ASA) is in base 64 encoded format.

Response

```
{
 "ret": "y",
 "code": "XXXXXXXXXXXXXXXXXXXXXXXXxxxx",
 "txn":   "XXXXXXXXXXXXXXXXXXXXXXXXXXX",
 "ts": "XXXXXXXXXXXXXXXXXXXXX",
 "err": "000",
 "errdesc": "",
 "rrn": "XXXXXXXXXXXXX",
 “ref”:”client-ref-data”,
 "responseXML": "Base64 encoded string”
}
```

Failure Response

```
{
 "ret": "n",
 "code": "XXXXXXXXXXXXXXXXXXXXXXXXxxxx",
 "txn":    "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
 "ts": "XXXXXXXXXXXXXXXXXXXXX",
 "err": "XXXXXXXXX",
 "errdesc":"XXXXXXXXXXXXX",
 "rrn": "XXXXXXXXXXXXXX",
 “ref”:”client-ref-data”,
 "responseXML": "Base64 encoded string"
}
```

Response Attributes

Attribute	Type	Description
ret	string	Result of OTP generation request. “y” if successful, “n” if failure
code	String	Unique alphanumeric “OTP response” code having maximum length 40.
txn	string	AUA specific transaction identifier.
ts	string	Timestamp when the response is generated
err	string	Failure error code, in case of success it is 000.
errdesc	string	Failure error description
rrn	string	Your request transaction ID
ref	string	Your Reference Data Sent in Request
responseXML	String	E-Kyc Response in Base64 Encoded XML format. Refer **Annexure B** for the format.

Annexure A

Error Codes:

1. Authentication

Error Code	Description
100	Pi (basic) attributes of Demographic data did notmatch
200	Pa (address) attributes of demographic data did not match
300	Biometric data did not match
310	Duplicate fingers used
311	Duplicate Irises used.Version 2.0.
312	FMR and FIR cannot be used in same transaction
313	Single FIR record contains more than one finger
314	Number of FMR/FIR should not exceed 10
315	Number of IIR should not exceed 2
316	Number of FID should not exceed 1
330	Biometrics locked by Aadhaar holder
400	OTP validation failed
402	txn value did not match with txn value used in Request OTP API
500	Invalid encryption of Skey
501	Invalid certificate identifier in ci attribute ofSkey
502	Invalid encryption of Pid
503	Invalid encryption of Hmac
504	Session key re-initiation required due to expiryor key out of sync
505	Synchronized Key usage not allowed for the AUA
510	Invalid Auth XML format
511	Invalid PID XML format
512	Invalid Aadhaar holder consent in rc attribute ofAuth
514	Invalid UID token in input.
515	Invalid VID Number in input.
517	Expired VID is used in input.
520	Invalid tid value
521	Invalid dc code under Meta tag
522	Invalid IDC code under Meta tag
523	Invalid CDC code under Meta tag
524	Invalid mi code under Meta tag
525	Invalid mc code under Meta tag
526	Invalid irmi code under Meta tag
527	Invalid mc code under Meta tag
528	Invalid fdmi code under Meta tag
529	Invalid fdmc code under Meta tag

530	Invalid authenticator code
540	Invalid Auth XML version
541	Invalid PID XML version
542	AUA not authorized for ASA
543	Sub-AUA not associated with AUA
550	Invalid Uses element attributes
551	Invalid tid value
552	Invalid value for wadh attribute within PID block
553	Registered devices currently not supported.
554	Public devices are not allowed to be used.
555	rdsId is invalid and not part of certification registry.
556	rdsVer is invalid and not part of certification registry.
557	dpId is invalid and not part of certification registry.
558	Invalid dih
559	Device Certificate has expired
560	DP Master Certificate has expired.
561	Request expired
562	Timestamp value is future time
563	Duplicate request (this error occurs when exactly same authentication request was re-sent by AUA)
564	HMAC Validation failed
565	AUA license has expired
566	Invalid non-decryptable license key. Version 2.0 (Rev 1) Aadhaar Authentication API© UIDAI
567	Invalid input
568	Unsupported Language
569	Digital signature verification failed
570	Invalid key info in digital signature
571	PIN Requires reset
572	Invalid biometric position
573	Pi usage not allowed as per license
574	Pa usage not allowed as per license
575	Pfa usage not allowed as per license
576	FMR usage not allowed as per license
577	FIR usage not allowed as per license
578	IIR usage not allowed as per license
579	OTP usage not allowed as per license
580	PIN usage not allowed as per license
581	Fuzzy matching usage not allowed as per license
582	Local language usage not allowed as per license
586	FID usage not allowed as per license.
587	Name space not allowed
588	Registered device not allowed as per license

590	Public device not allowed as per license
591	BFD usage is not allowed as per license //New
710	Missing Pi data as specified in Uses
720	Missing Pa data as specified in Uses
721	Missing Pfa data as specified in Uses
730	Missing PIN data as specified in Uses
740	Missing OTP data as specified in Uses
800	Invalid biometric data
810	Missing biometric data as specified in Uses
811	Missing biometric data in CIDR for the given Aadhaar number
812	Aadhaar holder has not done Best Finger Detection
820	Missing or empty value for bt attribute in Uses element
821	Invalid value in the bt attribute of Uses element
822	Invalid value in the bs attribute of Bio elementwithin Pid
901	No authentication data found in the request
902	Invalid dob value in the Pi element
910	Invalid mv value in the Pi element
911	Invalid mv value in the Pfa element
912	Invalid ms value
913	Both Pa and Pfa are present in the authenticationrequest
914	Face alone is of allowed as biometric modality. You should send face along with another biometric modality like Finger or IRIS or OTP.
915	Face auth is not allowed for this age of resident.
916	Invalid face Image format in input.
917	Invalid face capture type.
930	Technical error that are internal to authentication server
931	Technical error that are internal to authentication server
932	Technical error that are internal to authentication server
933	Technical error that are internal to authentication server
934	Technical error that are internal to authentication server
935	Technical error that are internal to authentication server
936	Technical error that are internal to authentication server
937	Technical error that are internal to authentication server
938	Technical error that are internal to authentication server
939	Technical error that are internal to authentication server
940	Unauthorized ASA channel
941	Unspecified ASA channel
950	OTP store related technical error
951	Biometric lock related technical error
980	Unsupported option
995	Aadhaar suspended by competent authority
996	Aadhaar cancelled

997	Aadhaar Suspended
998	Invalid Aadhaar Number
999	Unknown error

2. E-KYC

Error Code	Description
K-100	Resident authentication failed
K-200	Resident data currently not available
K-540	Invalid KYC XML
K-541	Invalid e-KYC API version
K-542	Invalid resident consent
K-543	Invalid timestamp
K-544	Invalid resident auth type
K-545	Resident has opted out of this service
K-546	Invalid value for pfr attribute
K-547	Invalid value for wadh attribute within PID block
K-550	Invalid Uses Attribute
K-551	Invalid Txn namespace (should be UKC)
K-552	Invalid license key
K-563	Duplicate request (this error occurs when exactly same authentication request was re-sent by AUA)
K-569	Digital signature verification failed for KYC
K-570	Invalid key info in digital signature for e-KYCXML
K-600	AUA is invalid or not an authorized KUA
K-601	ASA is invalid or not an authorized KSA
K-602	KUA encryption key not available
K-603	ASA encryption key not available
K-604	KSA not allowed to sign
K-605	Neither KUA key nor ASA encryption key are available
K-955	Technical Failure
K-999	Unknown error

3. OTP

Error Code	Description
110	Aadhaar number does not have verified mobile/email
111	Aadhaar number does not have verified mobile
112	Aadhaar number does not have both email and mobile
113	Aadhaar Number doesn’t have verified email ID.
114	Aadhaar Number doesn’t have verified Mobile Number
115	Aadhaar Number doesn’t have verified email and Mobile
510	Invalid OTP XML format

515	Invalid VID Number in input
517	Expired VID is used in input
520	Invalid device
521	Invalid mobile number
522	Invalid type attribute
523	Invalid ts atrribute. Either it is not in correct format or older than 20 min.
530	Invalid AUA code
540	Invalid OTP XML version
542	AUA not authorized for ASA
543	Sub-AUA not associated with AUA
563	Duplicate request (this error occurs when exactly same authentication request was re-sent by AUA)
565	AUA License key has expired or is invalid
566	ASA license key has expired or is invalid
569	Digital signature verification failed
570	Invalid key info in digital signature
940	Unauthorized ASA channel
941	Unspecified ASA channel
950	Could not generate and/or send OTP
952	OTP Flooding error //New
995	Aadhaar suspended by competent authority
996	Aadhaar cancelled
997	Aadhaar Suspended
998	Invalid Aadhaar Number
999	Unknown error

4. Other Error Codes

VE01	AUA Permissions Required.
VE02	KUA Permissions Required.
VE03	AUA/KUA Account Inactive.
VE04	Invalid AUACODE.
VE05	Invalid Request Type.
VE06	RequestType Error.
VE07	Invalid Request Length.
VE08	Signing Certificate Not Mapped.
VE09	Invalid Aadhaar Number.
VE10	Audit Logging in DB is failed for request.
VE11	Audit Logging in DB is failed for response.
VE12	ASA/KSA is unable to connect to UIDAI server.
VE13	Blank Response Received from UIDAI.
VE14	Response Signature Verification Failed.

VE15	Response XML Not Parsed Properly.
VE16	Duplicate Transaction ID.
VE99	KSA/ASA Internal Error.
VEA01	AUTH XSD Validation Failed.
VEA02	AUTH XML Not Parsed Properly.
VEA03	Blank AUTH XML Received from AUA.
VEA04	AUTH Signature Verification Failed.
VEA05	Invalid AUTH Version.
VEA06	Internal Error.
VEO01	OTP XSD Validation Failed.
VEO02	OTP XML Not Parsed Properly.
VEO03	Blank OTP XML Received from AUA.
VEO04	OTP Signature Verification Failed.
VEO05	Invalid OTP Version
VEO06	Internal Error.
VEK01	KYC XSD Validation Failed.
VEK02	KYC XML Not Parsed Properly.
VEK03	Blank KYC XML Received from AUA.
VEK04	KYC Signature Verification Failed.
VEK05	Invalid KYC Version.
VEK06	Internal Error.
VEB01	BFD XSD Validation Failed.
VEB02	BFD XML Not Parsed Properly.
VEB03	Blank BFD XML Received from AUA
VEB04	BFD Signature Verification Failed.
VEB05	Invalid BFD Version.
VEB06	Internal Error.
E-000	Request received is a HTTP request.
E-001	Request received is a get request.
E-100	AUTH XML Not Parsed Properly.
E-102	Audit Logging in DB is failed for request.
E-103	Audit Logging in DB is failed for response.
E-104	Audit Logging in DB is failed for Error occurred.
E-105	KYC XSD Validation failed
E-106	KYC Request signature verification failed.
E-107	AUTH Signature Verification Failed.
E-108	IP verification failed for entity.
E-109	Blank Response Received from UIDAI.
E-110	Unable to decrypt response at KSA
E-111	KYC response signature verification failed.
E-112	Auth Response Signature Verification Failed

E-113	BFD XSD Validation Failed.
E-114	OTP XSD Validation Failed.
E-115	AUTH response XML not parsed properly.
E-116	AUTH Response XML Not Parsed Properly.
E-117	Signed Auth XML Generation Error.
E-118	Auth Response Signature Verification Failed
E-119	ASA/KSA is unable to connect to UIDAI server.
E-120	Auth XSD Validation Failed.
E-121	Database audit logging in failed due to the duplicate transaction ID.
E-122	Property file unavailable.
E-123	BFD Request XML Not Parsed Properly.
E-124	OTP Request XML Not Parsed Properly
E-125	BFD Request Signature Verification Failed
E-126	OTP Request Signature Verification Failed
E-127	Signed BFD XML Generation Error.
E-128	Signed OTP XML Generation Error.
E-129	BFD Response XML Not Parsed Properly.
E-130	OTP Response XML Not Parsed Properly.
E-131	XML decryption error
E-132	Error during KYC request signature verification.
E-133	Error during KYC response signature verification.
E-134	Error during AUTH Request Signature Verification.
E-135	Error during AUTH Response Signature Verification.
E-136	Error during BFD Request Signature Verification.
E-137	Error during OTP Request Signature Verification.
E-138	Error during KYC XSD Validation
E-139	Error during AUTH XSD Validation
E-140	Error during BFD XSD Validation.
E-141	Error during BFDOTP XSD Validation.
E-142	Error during IP verification.
E-143	Response Received is E
E-144	BFD Response Signature Verification.
E-145	AUTH XSD Validation failed.
E-199	KSA/ASA Internal Error.
E-555	Duplicate Transaction Id Error.
S-100	Service Testing.

Annexure B

UIDAI Response XML Formats

Please refer to the UIDAI Technical Document in the below link for response xml formats.

https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf

https://uidai.gov.in/images/resource/aadhaar_ekyc_api_2_5.pdf

https://uidai.gov.in/images/resource/aadhaar_otp_request_api_2_5.pdf