



Fingpay Cash Deposit

API INTEGRATION DOCUMENTATION

AEPS CASH DEPOSIT API

Version 1.1

Date: 15.10.2024



IP must be whitelisted at Fingpay end before integration and this IP should not be white listed by another provider (shared IP across customers is not allowed)

1.API FOR CASH DEPOSIT(JAVA and PHP)

<https://fingpayap.tapits.in/fpaepsservice/api/CashDeposit/merchant/deposit>

<https://fingpayap.tapits.in/fpaepsservice/api/CashDeposit/merchant/php/deposit>

HEADERS :

trnTimestamp: In this field timestamp of the transaction must be sent. Format of the timestamp should be dd/MM/yyyyHH:mm:ss

hash : Generated JSON and also security key(**which is provided by fingpay**) must be encrypted using SHA-256 algorithm and converted to BASE64 which is to be sent in hash header

hash=SHA256(JSON+securitykey) // + means string concatenation

deviceIMEI : In case of web you need to send the scanner's serial number which is integrated in your system for performing transactions, based on the IMEI will assign the terminal.

eskey :

- First a session key is generated using AES-128 algorithm of the BC provider
- Session key is Encrypted using public key(**which is provided by Fingpay**) with the algorithm RSA/ECB/PKCS1Padding of BC provider
- Generated encrypted data must be converted to BASE64 which is to be sent in **eskey**.

superMerchantId: Should send the id of the supermerchant of the merchant which is passed during the transaction which is provided by Fingpay

Body:

- JSON is Encrypted using session key , generated while eskey generation.
- Generated encrypted data must be converted to BASE64 which is to be sent in **body**.

Sample Headers and Body :

```
trnTimestamp = 29/11/2017 15:24:47
hash = ixV3GdhMyrTm3aacQXRft1C8uL4doDUJVBWmSOL1vxc=
deviceIMEI = 352801082418919
eskey=cM1C5gd2ugAgcyDMNAHmW4cNeBHHxOfwZ7HvyNTD6l2MV09CIZVOEMT9uyfHtGLrco
DXD7V8M+ZeGSlvJ4sbedwJvTXr8wAHedfeZoHi4qUMXC8XFaoHrr+qYVc2+trJbGanY2e8pMLrPD
oTKrRh2NVwGBH+Z0VF5cV6aai2nLH4WdTV+EEYx+
superMerchantId=2
```

Body:

```
ngW07ebihM9cb4M8HeWVBnUohq81wLlwoVbIA7tTdfSCzceNoIDADOAfXaitH8WltONdJXiaUw
mKNZBCwnwVxm1e2eayJrEY8sNjyUWtVmOxXhefmDcK6/Hch4XwG9+Imzua2WiYQAoFq5+6+B2
tL2Lo5d60SOylFMjFBrU3szJcvW/8lftpgQENOOi7Z5sURbaXRak4hwqZnl5+piCaxDUgZ5qRJBZ1Xrg
OZcleP7LxEp3DcdnYYiDNDXPyCy9sb0Uoda72nFieQluwEE/VFlw04O7WwvFRhuWbMp/sPzPIVyw
wxft4xo2cbZPVBllZd2YvTDG1CVCSHGK6NPFOfKVatfUn+Jh/grBskNB0Gxy0JkvWnxdfyls5eSDiKVf
HLiCULdk8PB+kEE05XzaBt9NSC4EaL983xh512Ox6XF68IY+fSReap5rCGy4q7xLisZRZeKSNj4uZvZ5
xceb4JKNyHmyvDCfLJ1KkkGXrT/s9mo72dSI0mQTYlMkICjy+uUgbG4MYpzNsiNXtK+w/fZOzARYhs
KQbyum98Gx9ziHEVwHBkiT16RyhHwyrXXp5qjom0OKXePr/Weg8ukXbZBS/ =(This data is larger
than this example given)
```

PARAMETERS TO BE POSTED :

```
private P2CardnumberORUID cardnumberORUID;
private String mobileNumber;
private String paymentType;
private String timestamp;
private String transactionType;
private double latitude;
private double longitude;
private String requestRemarks;
```

```
private boolean isFacialTan;  
private boolean isIRISTxn;  
private String deviceTransactionId;  
private CaptureResponsecaptureResponse;  
private String languageCode;  
private double transactionAmount;  
private String merchantTranId;  
private String merchantUserName;  
private String merchantPin;
```

cardnumberORUID(Under cardnumber or uid there are 4 other parameters)

```
private String adhaarNumber;  
private int indicatorforUID;  
private String nationalBankIdentificationNumber;  
private String virtualId;(only if you are sending virtual id)
```

captureResponse(Under capture response below are the parameters)

```
private String errCode;  
private String errInfo;  
private String fCount;  
private String fType;  
private String iCount;  
private String iType;  
private String pCount;  
private String pType;  
private String nmPoints;  
private String qScore;  
private String dpID;  
private String rdsID;  
private String rdsVer;  
private String dc;  
private String mi;  
private String mc;  
private String ci;  
private String sessionKey;  
private String hmac;  
private String PidDatatype;  
private String Piddata;
```

(M) defines that that is mandatory field.

Parameter name	Description	Value(Mandatory/not)
----------------	-------------	----------------------

cardnumberORUID		
1.adhaarNumber	The Adhaar Number of Customer who is doing the transaction and it requires to be authenticated using an algorithm“ VerhoeffAlgorithm”	In case of virtual id the adhaar number by default it should be 999999999999(12 9's) constant value.otherwise it should be adhaar number of customer(M)
2.indicatorforUID	Values are defined by bank	It is constant(value is '0')in case of adhaar payment, in case of virtual id please send the value as '2'(M)
3.nationalBankIdentificationNumber	This is the selected bank by Customer forperforming the transaction.	The IIN list can be fetched from (ie, merchant bank details URL AEPS- https://fingpayap.tapits.in/fpaepsservice/api/bankdata/bank/details
4. virtualId	Virtual id of the customer and should be verified with verhoeff algorithm	Virtual id of the customer it should be 16 didgit value
5.mobileNumber	Mobile number of the customer	
6.paymentType	Unique code for different type of transactions	"B" (Constant for every transaction in aeps)(M)
7.transactionType	Type of the transaction	CD-cash deposit(M)
8.Latitude	Latitude of the place where transaction is happening	(M)
9.Longitude	Longitude of the place where transaction is happening	(M)
<u>10.requestRemarks</u>	If customer or merchant wants to send some remarks	
11.captureResponse	This response we receive it from the scanner dependent RDSERVICE , for any further information please refer the Scanner Dependent RD service documentation. These details will vary based on staging and production.	Should not change anything in capture response should send as it is.
12.transactionAmount	Amount of the transaction entered by	Amount of the

	customer or merchant	transaction
13.languageCode	Every language is defined with a code.	en is for english(M)
14.MerchantTranId	Client reference transaction id to check the transaction status. You must generate a unique merchantTransactionid every time while initiating a transaction.	(M)
15.timestamp	Timestamp of the transaction	(M)
16.merchantUserName	Username of the merchant which is registered under Fingpay as a merchant	(M)
17.merchantPin	Pin of the merchant who is onboarded.	Password must be MD5 hashed(M)
18.isFacialTan	True if it is facial authentication otherwise false	
19.isIRISTxn	True if it is iris authentication otherwise false	

SAMPLE JSON :

EncryptedJSON Payload for following plain sample JSON is to be sent

```
{
  "merchantTranId": "20171006100425",
  "captureResponse": {
    "PidDatatype": "X",
    "Piddata":
      "MjAxNy0xMC0wNlQxMDowNTowN3yUurFGz3Je+v4tjj64SRJwfxB5x5sayPZRqOOUX/EL4vzWh6
      R2XsObiujNTq12p8upDf7/teQ1LQCJKI8v3AlkiWsxOXOlnCSvsSV2KRudCz0eKgPRxAh13stb3ZSXhk
      ynkZl/qocKOR9BLHlhvgeCWg0cf/GTmgMiJL3KzSM7RRCw0zPkkcp2tT4X+7fqXMu1p6XSqmAC6U
      Pofw1KusKSavufd9CegyUNkK8X2iDUMkPt7DyZKSvEDfN8csOjHgqeFUCVUI40uSoMGsSJGH38qd
      M8Q3MNPYTqTuObuU9bFQsd0TerXptDmeMJN0+F9lI3p40b11riPUR4I7EwtuFg/JG/NBWeOJfI6
      Jexz0onK8Yys4eqq550f/WEVgh1AyyV32bsf8zVGKhqmLBWcvIVFdYaaDW+IKCOI7yreHCig3TBe+z
      bV06Ecsze9xdH5cy1o0gHRB2mAzLir+Eyqaln4aXEQ0dm2pwUjICKanSOVrYP2A6J7+bncxUMeZRI
      qB30aLNdrDLOsGNgrRM7aRRnlEX+aGsMQjKnpo9ZehWnVIXI3x2aMfwLXJ+QpCAelHSd3Q5Aik1
      ZLnFhRHxSP/qbAnfpelnMRz+AeKGDdbUuGdfJGzsfUhmzn5IstIjFJ0hliQrIIJdGyPL6+pJnKew+OifnP
      Nqi79nF/cAk7WKJr+yAhzPOYU4gsb+tx3d/lzkn+UiXaUpzEikBTfJ+VJ9rG1d+IJTlzmZrDxOhkDY7Z
      WB9YSLtKcaZAnc2IqRvSi+FXmXm/4vsyYUPLrw+rmFRwqQtzMSThEC3lxWZQXlxyA0N5EGujMoG
      EZIAle6uqfG6RhguDgVJqCbR4BoVIOOYcQipoS7wKMyQdtfhVORkotV4x7hH1bXyyf7eekocfpSzs
      RUvzSU+3YAUi89neOdaHMcL9jPGncG9AKtL8hVr0wF7iwl+f9OdIh1ubUHKO+29xrCizELa21wdVm
      mKfLlJVU2YEjFmFDu4Ozl6eTEPTQLaysrJHSSu/DHadWXg4FHTL+j5RaRIba41bbUOR+9caWz5bDOi
      p+vsSUNoGVUC6XBNYgiFy9Kj6Dy1B1zizGEDqd/DkSRONk1ISqOmWnTsUfWX9CwokI5Ho1bqodK
      ZrA1Ng/ozNcpVMNLxVagi3PWztEqbVjAQydGbBJXaQ6c4HcQ2D5Xqtuml4uZUt8d6XOR2W58mZ
```

9cWk17gCfoT0M3kn8zlbrPTnAoFfvFcR4wOox1dwj4Q1I/k29ktpVwEMLGVytR1jB+zysbE+IKnRb4/b9PYSQXxURFpyyESZtszM3xwyBBCBgIWspNeysT1xM/KA\u003d\u003d",

"ci": "20191230",

"dc": "83017feb-b271-460b-92e8-6e12a3a0189e",

"dpiD": "PRECISION.PB",

"errCode": "0",

"errInfo": "Image Capture Success",

"fCount": "1",

"fType": "0",

"hmac": "9ZqjrXUjxGTSQsngxUHDpBYqBhOBNARldRKMhHCq7c+yImkLOxMkSQBWmihMPrx3",

"iCount": "0",

"mc":

"MIIEBDCCAuygAwIBAgIIfc0if0pbK5gwDQYJKoZIhvcNAQELBQAwdgxNzA1BgNVBAMTLkRTIFByZWNpc2lvbiBCaW9tZXRYaWMgSW5kaWEgUHJpdmF0ZSBMaW1pdGVkIDExIzAhBgNVBDMTGjlyIEhhYmlidWxsYWggUm9hZCBUIE5hZ2FyMRAwDgYDVQQJEwdDaGVubmFpMRIwEAYDVQQQEwIU YW1pbG5hZHUxETAPBgNVBAsTCFNVZnR3YXJIMTIwMAYDVQQKEylQcmVjaXNpb24gQmlvbWV0 cmljIEluZGhIFByaXZhdGUtGltXRIZDELMakGA1UEBhMCSU4wHhcNMTcxMDA1MDkzNDU2W hcNMTcxMTA0MDkzNDU2WjBuMTIwMAYDVQQKDClQcmVjaXNpb24gQmlvbWV0cmljIEluZGhIF ByaXZhdGUtGltXRIZDESMBAGA1UECwwJQmlvbWV0cmljMRAwDgYDVQQQHDAAdSEVOTkFj MRIwEAYDVQQQDDAIQcmVjaXNpb24wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC OGiyIA1TyPN3tUU+wx/s4hAT6OHhpJS+61dz3k4ihXIBTgmWJs5NddO4HjpT8FI3z0SQn6aykOMzH gBpiznj2sgv9iioKzGntqZo0LJdBNJ2997cf7mNIEeMaZXdQhMKQU7Xff9pDT074U/ygJ7OtXqK1jW db+OhAY0V0sTTXFSiTSuk2YziL3MFWS1aHILU5N7I6h9CqyztoiGwn5d/1rbTk3/KdrllwziYUBZZ9CK 8PCc/oiIIEBD9oDg/CK2H+KkpKChMsXzOv0B9KvsW12iWvgrLhPYHtU+ni7465EVvYPCsYOxev1qQ qs4B2GVEcXo6kyQLqgjx4wlcGLHx5AgMBAAGjOzA5MAkGA1UdEwQCMAAwCwYDVROPBQAQDAg GGMB8GA1UdIwQYMBaAFLU1sKRXC/kwcet03DIXvSifcyhnMA0GCSqGSIb3DQEBCwUAA4IBAQB FsnoA2UtugIE+kKwY3GdUIKv6bj0oyhbaHFwi8ewR/WI1abdertApefLmk0Aa+5PFya+KaZCWkZIDK ORI1J1624yXS+Yh3NnbWOieBKfeax31h6peytMgd85adqxhiEowYTHWJ/PkSku+AFGieMILtZDIcy/C Vvs5I4CcHvjLsrhdowwOUli4v1OS9zKaRgwp/bzhP0ZuDW7JjaqzFIKwwbi+6cs3HLPvTBAGeED5Oe wFsTxaZnJa0Skqgoi0VQYlurRf50AOG3/bP0Osh6MWylQZRluNI3A7jxz3sDqsBW+weIq4Qj8A5d97 /7ctQNKe6/PGVpNop3W2dgJS9Fut",

"mi": "PB400",

"nmPoints": "46",

"pCount": "0",

"pType": "0",

"qScore": "100",

"rdsID": "PRECISION.AND.101",

"rdsVer": "1.1.0",

"sessionKey":

"M1++JGFa/Vp4szTGOFK0G3NNsVqGoOffD4xnBf5QZO8TKO02ap9eWN6ZpTcXrkM+VlyJ0DZkQf CcrjlcAlh49Mw9a6wcipIJ0IS+wGN6szA1LH85c7Ciem/HNVGW7GH9u21cfSpnEmXIBKtfd5IULTnO VPF7PufufgFCXC3rSsX8zWOogbEZmKP6eiyw3+gqRb10NyKn90qJGLioBcMaNPt32r5kW2ppne07A TQLuWZqLdhzVX1tHimCTjm5NchQIAFjrjBKWxVGdEIZ44VJEEeyTa+A6J/Fp4n/8whidnYob+XKQ8/ PvEsu6oSXRwiL1N7QGp8RP48+S57mzlwlw\u003d\u003d"

```
},  
  
"cardnumberORUID": {  
  "adhaarNumber": "123443211234",  
  "indicatorforUID": 0,  
  "nationalBankIdentificationNumber": "607152"  
},  
  
"languageCode": "en",  
"latitude": 13.0641367,  
"longitude": 80.2480973,  
"mobileNumber": "9952396587",  
"paymentType": "B",  
"requestRemarks": "TN3000CA0006530",  
"timestamp": "06/10/2017 10:05:24",  
"transactionAmount": 1.0,  
"transactionType": "CD",  
"merchantUserName": "sai",  
"merchantPin": "81DC9BDB52D04DC20036DBD8313ED055"  
}
```

RESPONSE PARAMETERS :

```
private boolean status;  
private String message;  
private Object data;  
private long statusCode;
```

data :

```
private String terminalId;  
private String requestTransactionTime;// dd/MM/yyyyHH:mm:ss  
private double transactionAmount;  
private String transactionStatus;  
private double balanceAmount;  
private String bankRRN;  
private String transactionType;  
private String fpTransactionId;  
private String merchantTxnId;
```


Parameter name	Description
terminalId	Terminal assigned while performing a transaction
requestTransactionTime	Requested timestamp of the transaction
transactionAmount	Amount entered by the customer
transactionStatus	Status of the transaction either success or false
balanceAmount	Balance amount of the customer in his account which we receive in response from the bank
bankRRN	Unique id generated by bank which we will receive in the response from bank
transactionType	Transaction type sent by client
fpTransactionId	Transaction id generated by Fingpay
merchantTxnId	Merchant transaction id sent by client
errorCode	Error code received from bank in response in case of failure
errorMessage	Error message will be fetched from the table

SAMPLE RESPONSE:

```
{
  "status":false,
  "message": "Issuer bank down",
  "data": {
    "terminalId": "FA09778",
    "requestTransactionTime": "01/01/2018 23:59:59",
    "transactionAmount": 100.0,
    "transactionStatus": "failed",
    "balanceAmount":0 .0,
    "bankRRN":"765765656857" ,
    "transactionType": "CD",
    "errorMessage": "Issuer bank down",
    " fpTransactionId ": "CD00010291117175529",
    "merchantTxnId":"123221",
    "responseCode": "00",
    "stan": "022823",
  },
  "statusCode": 10000
}
```

SAMPLE FAILURE RESPONSE:

```
{
  "status": true,
  "message": "Request Completed",
  "data": {
    "terminalId": "FA09778",
    "requestTransactionTime": "01/01/2018 23:59:59",
    "transactionAmount": 101.0,
    "transactionStatus": "successful ",
    "balanceAmount": 200.0,
    "bankRRN": "765765656857",
    "transactionType": "CD",
    "errorMessage": "Success",
    "fpTransactionId": "CD00010291117175529",
    "merchantTxnId": "123221",
    "responseCode": "0U28",
    "stan": "022823",
  },
  "statusCode": 10004
}
```

4.STATUS CHECK:

STATUS CHECK FOR CASH DEPOSIT:

URL:

<https://fingpayap.tapits.in/fpaepsweb/api/auth/merchantInfo/statusCheckV2/merchantLoginId/cashDeposit>

Request object:

```
private String merchantTranId ;

private String hash;

private String merchantLoginId;
```

Parameter name	Description	Value of the parameter
merchantTranId	This is your reference transaction id for you to check the transaction status. You must generate a unique merchantTxnId every time you are initiating a transaction.	It can be anything which is unique for every transaction(integer and alphabet)
merchantLoginId	Login id of the merchant who is doing the transactions and already registered in the Fingpay system	Loginid of the merchant whose transactions you want to status check.
merchantpassword	Merchant password is the pin of merchant	It should be md5 hashed and used in generation of hash which is provided by fingpay team.

Hash generation logic:

```
hash =base64.encode(SHA256(concat(Merchanttransactionid,+,MD5(merchantPassword))))
```

- Concatenate the merchanttransactionid,"+" symbol and merchant password which must be encrypted using MD5 hash, this generated string must be encrypted using SHA-256 algorithm and converted to BASE64 which is to be sent in hash header

Sample Request

```
{
"merchantLoginId": "Fingpay",
"merchantTranId":"636838180887166778",
"hash":"taLwRIIn+bF9q+T9NFFipFbxKAusdOOWM1lhJ6KMmC10="
}
```

Response Object:

```
private booleanapiStatus;
```

```
private String apiStatusMessage;  
private Object data;  
private long apiStatusCode;
```

data:

```
private String fingpayTransactionId ;  
private String stan ;  
private String bankRRN ;  
private String transactionTime;  
private String merchantTranId ;  
private boolean transactionStatus;  
private Double transactionAmount;  
private String transactionStatusCode;  
private String transactionStatusMessage;  
private String remarks;  
private double balanceAmount;  
private String aadhaarNumber;  
private double latitude;  
private double longitude;  
private String mobileNumber;  
private String deviceIMEI;  
private String bankName;
```

Parameter name	Description
remarks	Remarks if anything sent while doing transaction will be posted back

TransactionTime	Requested timestamp of the transaction
transactionAmount	Amount entered by the customer
transactionStatusCode	Status of the transaction either success or false
bankRRN	Unique id generated by bank which we will receive in the response from bank
stan	Unique id of the transaction generated by fingpay
fingpayTransactionId	Transaction id generated by Fingpay
merchantTranId	Merchant transaction id sent by client
Transaction statusMessage	Error message corresponding to the error codes are sent
TransactionStatusCode	Depending on the transaction error codes will be sent
balanceAmount	Balance amount of the customer in his account which we receive in response from the bank(You should format it last two digits are paise
Aadhaar number	Aadhaar number of the customer
latitude	Latitude where the transaction initiated
longitude	Longitude where the transaction initiated
Mobile number	Mobile number of the customer
deviceIMEI	IMEI of the device where transaction initiated
bankName	Customer bank name for the transaction

Sample Success Response

```
{
  "apiStatus": true,
  "apiStatusMessage": "Request Completed",
  "data": [
    {
```

```
"fingpayTransactionId": "CDB141217091916190021",  
  "stan": "109983",  
  "bankRRN": "926016231481",  
  "transactionTime": "17-Sep-2019 16:19:00",  
  "merchantTranId": "1851501043",  
  "transactionStatus": true,  
  "transactionAmount": 10000,  
  "transactionStatusCode": "00",  
  "transactionStatusMessage": "Success",  
  "remarks": null,  
  "balanceAmount": 409000,  
  "aadhaarNumber": "xxxxxxxx8869",  
  "latitude": 18.5229312,  
  "longitude": 73.62478080000001,  
  "mobileNumber": "9130460773",  
  "deviceIMEI": "000016461462456",  
  "bankName": "Union Bank of India"  
}  
],  
"apiStatusCode": 10000  
}
```

Sample Failure Response :

```
{
```

```
"apiStatus": false,  
"apiStatusMessage": "No data available for the requested data.",  
"data": null,  
"apiStatusCode": 0  
}
```

*** API will return "transactionStatusCode": "FP009" for "Transaction Response pending" when there is no response for the particular where you need to do status check of the transaction again**

*** We are making the transaction successful if the transaction is timeout and also in the case of 91,52,08 response code. we are storing the transaction response as 00 and response message as Deemed Success , but aggregator will get the response as 00 and success**

*** In such above cases, the customer may receive the amount in TAT of Max. T+5 days**

Response Code	Description
00	Success/Approved
91	Issuer is inoperative/ISSUER RESPONDED WITH RC-91 (timeout)
52	No checking Account
08	Issuer un-available / Issuer CBS Un-available

Note: NPCI currently maintains a 30-minute cooling period between Cash Withdrawal & Cash Deposit transactions to avoid round-tripping transactions

UIDAI Response Codes:

Response code	Description
00	APPROVED
KK	NUMBER OF BIOMETRIC MODALITIES SHOULD NOT EXCEED 2
KP	INVALID SUB AUA code
KS	BFD TRANSACTION SHOULD NOT CONTAIN OTHER IN INPUT
KT	AADHAAR LOCKED BY AADHAAR NUMBER HOLDER FOR ALL MODALITIES AUTHENTICATIONS
KU	AADHAAR NUMBER USAGE IS BLOCKED BY AADHAAR NUMBER HOLDER
KV	BFD USAGE NOT ALLOWED AS PER LICENSE
KW	Face alone is not allowed as biometric modality
KX	Face auth is not allowed for this age of resident
KY	Invalid face Image format in input
KZ	Invalid face capture type
M4	NRE ACCOUNT
M6	LIMIT EXCEEDED
OM	EXPIRED VID IN INPUT
UA	INVALID DEMOGRAPHIC DATA
UB	MISSING PI DATA AS SPECIFIED IN USES
UC	MISSING PA DATA AS SPECIFIED IN USES
UD	MISSING PIN DATA AS SPECIFIED IN USES
UE	UNKNOWN ERROR
UF	MISSING OTP DATA AS SPECIFIED IN USES
UG	INVALID BIOMETRIC DATA
UH	MISSING BIOMETRIC DATA SPECIFIED IN USES
UI	UIDAI TIME OUT
UJ	Missing PFA data specified in USES
UK	MISSING VALUE FOR BT ATT IN USES ELEMENT
UL	INVALID VALUE IN BT ATT IN USES ELEMENT
UM	NO AUTH FACTORS FOUND IN AUTH REQUEST
UN	INVALID DOB VALUE IN PI ELEMENT
UO	INVALID MV VALUE IN PI ELEMENT
UP	INVALID MV VALUE IN PFA ELEMENT
UQ	INVALID MS VALUE
UR	BOTH PA AND PFA ARE PRESENT
US	TECH ERROR 1-RELATED TO ABIS INTERACTION

UT	TECH ERROR 2- UID DB SERVER DOWN
UU	TECH ERROR 3 - XML ERROR
UV	UNSUPPORTED OPTION
UW	TRANSACTION AMOUNT EXCEED LIMIT
UY	INVALID PID XML FORMAT

UX	REQUEST OLDER THAN 24 hours
UZ	UNAUTHORIZED ASA CHANNEL
U0	UNSPECIFIED ASA CHANNEL
U1	PI BASIC ATTR DEMOGRAPHIC DID NOT MATCH
U2	PI ADDRESS ATTR DEMOGRAPHIC NOT MATCH
U3	BIOMETRIC DATA DID NOT MATCH
U4	INVALID ENCRYPTION
U5	INVALID XML FORMAT
U6	INVALID DEVICE
U7	INVALID AUTHENTICATOR CODE
U8	INVALID Auth XML VERSION
U9	INVALID USES ELEMENT ATTRIBUTES
VA	PIN RETRIES RESET
VB	INVALID BIOMETRIC POSITION
VC	PI USAGE NOT ALLOWED AS PER LICENSE
VD	PA USAGE NOT ALLOWED AS PER LICENSE
VE	PFA USAGE NOT ALLOWED AS PER LICENSE
VF	FMR USAGE NOT ALLOWED AS PER LICENSE
VG	FIR USAGE NOT ALLOWED AS PER LICENSE
VH	IIR USAGE NOT ALLOWED AS PER LICENSE
VI	OTP USAGE NOT ALLOWED AS PER LICENSE
VJ	PIN USAGE NOT ALLOWED AS PER LICENSE
VK	FUZZY USAGE NOT ALLOWED AS PER LICENSE
VL	LOCAL LANGUAGE USAGE NOT ALLOWED AS PER
VM	TECHNICAL ERROR
VN	TECHNICAL ERROR
VO	TECHNICAL ERROR
VP	TECHNICAL ERROR
VQ	TECHNICAL ERROR
VR	TECHNICAL ERROR
VS	Missing Biometric data in UIDAI CIDR
VT	Invalid certificate identifier in “ci” attribute of “Skey”
VU	INVALID ENCRYPTION OF PID

VV	INVALID ENCRYPTION OF HMAC
VW	AUA NOT AUTHORIZED FOR ASA
VX	SUB-AUA NOT ASSOCIATED WITH "AUA"
VY	INVALID PID XML VERSION
VZ	Duplicate Irises used
V0	REQUEST EXPIRED
V1	INVALID TIME STAMP
V2	Duplicate Request
V3	HMAC VALIDATION FAILED
V4	AUA license key expired
V5	ASA license key expired

V6	INVALID INPUT
V7	UNSUPPORTD LANGUAGE
V8	DIGITAL SIGNATURE VERIFICATION FAILED
V9	INVALID KEY INFO IN DIGITAL SIGNATURE
W0	FMR & FIR IN 1 TXN
W1	MORE THAN ONE FINGER IN SINGLE FIR
W2	FMR/FIR EXCEED 10
W3	IIR SHDNT EXCD 2
W4	SESSION KEY EXPIRE
W5	BEST FNGR DTCTN NOT DONE
W6	DUPLICATE FING USED
W7	INVALD PIN CODE
W8	INVALID GEO CODE
W9	OTP VALIDATION FAILD
WA	BIOMETRICS LOCKED
WB	Number of FID should not exceed 1
WC	"txn" value did not match with "txn" value used in Request OTP API
WD	Invalid resident consent in "rc" attribute of "Auth"
WE	Invalid "tid" value.
WF	Invalid mi code under Meta tag
WG	rdsId is invalid and not part of certification registry
WH	rdsVer is invalid and not part of certification registry
WI	Invalid mc code under Meta tag
WJ	Registered devices currently not supported
WK	Public devices are not allowed to be used
WL	FID usage not allowed as per license
WM	Name space not allowed

WN	Registered device not allowed as per license
WO	Public device not allowed as per license
WP	Invalid value in the “bs” attribute of “Bio” element within “Pid”
WQ	OTP store related technical error
WR	Biometric lock related technical error
WS	Aadhaar suspended by competent authority
WT	Aadhaar cancelled
WU	dpId is invalid and not part of certification registry
WV	Invalid dih
WW	WADH validation fail in RD
WX	Device Certificate has expired
WY	DP Master Certificate has expired
WZ	Technical error
X1	SYNC KEY USE NOT ALLOWED
X2	INVALID FNDR DEVICE
X3	INVALID IRIS DEVICE
X7	AADHAR NO STST LOST/DECEASED/NOT ACT

X8	AADHAR NO DOSENT EXIST IN CIDR
X9	Aadhaar Cancelled due to various reasons
XA	Invalid Protobuf Format
XB	Maximum number of attempts for OTP match is exceeded or OTP is not generated. Please generate a fresh OTP and try to authenticate again
XC	Invalid/Non Decryptable ANCS Token in input. Use a correctDANCS token.
XD	ANCS Token in input is already used or expired
XE	In appropriate ANCS token used. This means that the ANCS token used is not associated with the AUA or with theDtransaction ID
XF	VID is not yet generated. To use specific services like UID lockwhich require VID to be pre generated, please generate a VID before using service.
XG	Device blocked for more than allowed error percentage
XH	Device blocked for more than allowed velocity
XI	Face alone is of allowed as biometric modality. You should send face along with another biometric modality like Finger orDIRIS or OTP.

XJ	Face auth is not allowed for this age of resident
XK	Invalid face Image format in input
XL	Invalid face capture type
Y1	Device key rotation related issue
Z1	invalid UID token in input
Z2	Invalid VID Number in input
SA	Minimum signatory names not present
03	invalid merchant
05	Do not honor
08	Issuer un-available / Issuer CBS Un-available
12	Invalid transaction
13	Invalid amount
20	Issuer Decline – Unspecified reason
22	Reversal by acquirer terminal
30	Format Error
40	Reversal By NPCI not acknowledged by issuer
41	Reversal by acquirer not acknowledged by issuer
51	Insufficient funds
52	No checking account
53	No savings account
57	FREEZE/FROZEN ACCOUNT
59	Suspected fraud
61	Exceeds withdrawal amount limit
65	Exceeds withdrawal frequency limit
68	Response received too late
71	Deemed Acceptance
72	Version not supported by Issuer
76	Unable to locate BAV for CDA
90	Cut-off in process
91	Issuer is inoperative/ISSUER RESPONDED WITH RC-91
92	Unable to route transaction
94	Duplicate transaction
96	System malfunction
99	Declined