TWO FACTOR BIOMETRIC AUTHENTICATION API

VERSION :2.1.0

Date : 14/07/2023

Two Factor Authentication:

For java and .net

URL:https://fingpayap.tapits.in/fpaepsservice/auth/tfauth/merchant/validate/aadhar

UAT URL:https://fpuat.tapits.in/fpaepsservice/auth/tfauth/merchant/validate/aadhar

For PHP

URL:https://fingpayap.tapits.in/fpaepsservice/auth/tfauth/merchant/php/validate/aadhar
UAT URL:https://fpuat.tapits.in/fpaepsservice/auth/tfauth/merchant/php/validate/aadhar

For Simple API without encryption

URL:https://fingpayap.tapits.in/fpaepsservice/auth/tfauth/merchant/simple /validate/aadhar
UAT URL **:** https://fpuat.tapits.in/fpaepsservice/auth/tfauth/merchant/simple /validate/aadhar

Note:For simple API there are no only hash and trnTimestamp headers and body should be in plain json format

- Json+secretkey+trntimestamp this string must be encrypted using SHA-256 algorithm and converted to BASE64 which is to be sent in hash header

HEADERS :

trnTimestamp: In this field timestamp of the transaction must be sent.

hash : Generated JSON must be encrypted using SHA-256 algorithm and converted to BASE64 which is to be sent in hash header

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**.

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=cM1C5gd2ugAgcyDMNAHmW4cNeBHHxOfwZ7HvyNTD6l2MV09ClZVOEMT9uyfHtGLrco
DXD7V8M+ZeGSIvJ4sbedwJvTXr8wAHedfeZoHi4qUMXC8XFaoHrr+qYVc2+trJbGanY2e8pMLrPD
oTKrRh2NVwGBH+Z0VF5cV6aai2nLH4WdTV+EEXy+FTf3B1DzPqybSuP1Upe76VQNLXYQrdbp28n
Dvewk2dyBgKFHCmp26eNtZ0RaH3upbMoqHxPWhCgk/6cjD0Gx73zXVKSv/k1IhB9kD1n8qW77h
bLGKqNFZSaABk3OcfprFNY5Xpu53jhn/3E8jlSWF080AwWF08RRqBiWucFMPvACWc0Xiic+ei6ZW
KOGcfKIn1ZWZrPHFJlckO0TAZOTr47Jk18oIrGYp86lBfOT/EC8z3zKPCQn2woryhCWrGyZxXtPWQ7
EniBLUKRU1TUwkfEkeB/uG9zFL3Nl3lTK0y5ejwk3UDggygv4Y/3GjB1AtXHZT9j7D20CFT/JTUI/J1u
pu1ADMaH+ndWNKYDj6JH0V2i9jHb7wWoAnQbkcy7ywFTPX5O/E6oFi0Tb5xOHxxUxFD6sd2gu8
gwos6N5ijetFSST2i+5NzVYEDurlCfr7cupcdiTMjb0Oqrv5ouCVGMA/jw2WcYu0aT3ZlBgpyk=

Body:

ngW07ebihM9cb4M8HeWVBnUohq81wLIwoVbIA7tTdfSCzceNoIDADOAfXaitH8WItONdJXiaUw
mKNZBCwnwVxM1e2eayJrEY8sNjyUWtVmOxXhefmDcK6/Hch4XwG9+Imzua2WiYQAoFq5+6+B2
tL2Lo5d60SOyIFMjFBrU3szJcvW/8IftpgQENOoi7Z5sURbaXRak4hwqZnl5+piCaxDUgZ5qRJBZ1Xrg
0ZcIeP7LxEp3DcdnYYiDNDXPyCy9sb0Uoda72nFieQluwEE/VFlw04O7WwvFRhuWbMp/sPzPIVyw
wxFt4xo2cbZPVBllZd2YvTDG1CVCShGK6NPFOfKVaTfUn+Jh/grBskNB0Gxy0JkvWnxdfyls5eSDiKVf
HLiCULDk8PB+kEE05XzaBt9NSC4EaL983xh512Ox6XF68IY+fSReap5rCGy4q7xLisZRZeKSNj4uZvZ5
xceb4JKnYHmyvDCfLJ1KkkGXrT/s9mo72dSl0mQTYlMkICjy+uUgbG4MYpzNsiNXtK+w/fZOzARYhs
KQbyum98Gx9ziHEVwHBkiT16RyhHwyrXXp5qjom0OKXePr/Weg8ukXbZBS/aFeL42reRQ54CB1IF
eM2o930t/aR24roCIMHbOgArBzijqWxO21Ha2dpPtOFo5nTC2Vs800ufXQZmzQHt/rvRRrQvzXaf/
Nuk8j3G4AHNTGEM+Kv/8sfvKkRmJJAj6A1hnm4av10Ux9I/XK4OYCWzHY0xST6rE6cnsV2wm/IwG
ajn0TwSBkj0YLexCZGN7CXgOD5WCMM5sTp77o2khvXk58ZO337tjSMHk3HaLRAiqHnZCNxaelpN
TGpibNF4BrpBTr0ztaKXRQEZ1rEF87W531UoaIrib/BI0TIlgcE2KLrHA31wcoGU5n6b+uCk+pZ1KXP
UcrCySFDhBXuYD/DigbzDuZb2iAjdktee7Ur+JHYQTkNKE20/Mc5Gz98uvyZc+X6HpLcKOF7tRtVlsP
mdEavDo0raCJyf+7Jw2kZkpahYO64RjBFyxWbDbr38KpirYsKXEXiXfY2ZEX6jShpIX/qu08Aya2iPzDp

zq+CNG0GpiPmRwIgjEOD5xnCoUnOJtTXfqpbAFTAU630T8tKx6KPJNosnI8qXeZptYEMsVGjJwhgja
538ehFXVEtka/Wg6hipJAKh9nRQqhaUpBixDbXK/DvJiMR4Gh5DFqQSK2VLfW6CcQmTIJ8rVEGniX
ZsDfW+egRgmMR1UOwtfNevTn2ljYpx2kT+0FNBVniQ4C5r6mLsIQ6WulgZPUguQWOOmR2d72G
xO/TFbw5rRgKDoS7qamGbQsu0YZwgXkHcjm1bgKWXM7D/475gq/++Fh/GKO/c22HutDUWi6NJ
HkYfDBP+IjXeyKksU1uPy8Tut6qjOnczDFryYL4B62nqlY4IWkbjvqJT3Sr7p5jHsFdX6weHSjw86Awx
udnW91OnrbmYi1tNwBoHNKV3NzieKJ+myrZDbEMIsahD1rDYF7kOnub3kJ4SHKXv3mxoUHvnch
qJNCmQhPJ0+Ds+ZGk0sDkGu8vxdFperA8twSBCHs4pdM4DBD61nUk21HUaFaq7rNRfWUa9yKGj
ow7wsdKi/GGy2iW9g7JTQmWBZ8elh4QOQFzOvXeJ=(This data is larger than this example given

PARAMETERS TO BE POSTED :

```
private int superMerchantId;
private String merchantUserName;
private String merchantPin;
private String transactionType;// auth otp - AUO
private double latitude;
private double longitude;
private String requestRemarks;
private String merchantTranId;
private String serviceType ;// supports only AEPS or AP
private String mobileNumber;
private P2CardnumberORUID cardnumberORUID;
private CaptureResponse captureResponse;
```

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

```
private String adhaarNumber;
private int  indicatorforUID;
private String nationalBankIdentificationNumber;
```

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;
```

SAMPLE REQUEST :

Encripted JSON Payload for following plain sample JSON is to be sent


```
{
 "captureResponse": {
  "PidDatatype": "X",
  "Piddata":
"MjAxNy0xMC0wNlQxMDowNTowN3yUurFGz3Je+v4tjj64SRJwfxB5x5sayPZRqOOUX/EL4vzWh6
R2XsObiujNTqI2p8upDf7/teQ1LQCJKl8v3AlkIWsXOXOlnCSvsSV2KRudCz0eKgPRxAh13stb3ZSXhk
ynkZl/qocKOr9BLHIhvgeCWg0cf/GTmgMiJL3KzSM7RRCw0zPkkcp2tT4X+7fqXMu1p6XSqmAC6U
Pofw1KusKSavufd9CegyUNkK8X2iDUMkPt7DyZKSvEDfN8csOjHgqeFUCVUI40uSoMGsSJGH38qd
M8Q3MNPyTqTuObuU9bFQSd0TerXptDmeJMJNx0+F9ll3p40bI1riPUR4I7EwtuFg/JG/NBWeOJfI6
Jexz0onK8YYs4eqq550f/WEVgh1AyyV32bsf8zVGKhqmLBWcvlVFdYaaDW+lKCOI7yreHCig3TBe+z
bV06Ecsze9xdH5cy1o0gHRB2mAzLir+EyqaIn4aXEQ0dm2pwUjlCKanSOVrYP2A6J7+bncxUMeZRI
qB30aLNdrDLOsGNgzrRM7aRRnlEX+aGsMQjKnpo9ZehWnVlXl3x2aMfwLXJ+QpCAelHSd3Q5Aik1
ZLnFhRHXsP/qbAnfpelnMRz+AeKGDdbUuGdfJGzsfUhmzn5IstIjFJ0hliQrIlJdGyPL6+pJnKew+OifnP
Nqi79nF/cAk7WKJr+yAhzPOYu4gsb+tx3d/lzkn+UiXaUpzEikBTfJ+VJ9rG1d+IJTZlmzYrDxOhkDY7Z
WB9YSLtTkcaZAnc2IqRvSi+FXmXm/4vsyYUPLrw+rmFRwqQtzMSThEC3lxWZQXlxyA0N5EGujMoG
EZIAle6uqfG6RhguDgVJqCbR4BoVlOOYcQipoS7wKMyQdtfhVORkotV4x7hH1bXyyf7eekocfpSzsu
RUVzSU+3YAUi89neOdahMcL9jPGncG9AKtL8hVr0wF7iwI+f9OdIh1ubUHkO+29xrCizELa21wdVm
mKfLIjVU2YEjFmFDu4Ozl6eTEPTQLaysrJHSSu/DHadWXg4FHTL+j5RaRIba41bbUOR+9caWz5bDOi
p+vsSUNoGVUC6XBNYgiFy9Kj6Dy1B1zizGEDqd/DkSROnK1lSqOmWnTsUfWX9CwokI5Ho1bqodK
ZrA1Ng/ozNcpVMNLxVagi3PWztEqbVjAQydGbBJjXaQ6c4HcQ2D5Xqtuml4uZUt8d6XOR2W58mZ
9cWk17gCfoT0M3kn8zIbprPTnAoFfvFcR4wOox1dwj4Q1Il/k29ktpVwEMLGVytR1jB+zysbE+IKnRb
4/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": "9ZqjrXUjxGTSQsxgUHDpBYqBhOBNARldRKMrHCq7c+yImlkLOxMkSQBWmihMPrx3",
   "iCount": "0",
   "mc":
"MIIEBDCCAuygAwIBAgIIfc0if0pbK5gwDQYJKoZIhvcNAQELBQAwgdgxNzA1BgNVBAMTLkRTIFBy
ZWNpc2lvbiBCaW9tZXRyaWMgSW5kaWEgUHJpdmF0ZSBMaW1pdGVkIDExIzAhBgNVBDMTGjIyI
EhhYmlidWxsYWggUm9hZCBUIE5hZ2FyMRAwDgYDVQQJEwdDaGVubmFpMRIwEAYDVQQIEwlU
YW1pbG5hZHUxETAPBgNVBAsTCFNvZnR3YXJlMTIwMAYDVQQKEylQcmVjaXNpb24gQmlvbWV0
cmljIEluZGlhIFByaXZhdGUgTGltaXRlZDELMAkGA1UEBhMCSU4wHhcNMTcxMDA1MDkzNDU2W
hcNMTcxMTA0MDkzNDU2WjBuMTIwMAYDVQQKDClQcmVjaXNpb24gQmlvbWV0cmljIEluZGlhI
FByaXZhdGUgTGltaXRlZDESMBAGA1UECwwJQmlvbWV0cmljMRAwDgYDVQQHDAdDSEVOTkFJ
MRIwEAYDVQQDDAlQcmVjaXNpb24wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC
OGiylA1TyPN3tUU+wx/s4hAT6OHhpJS+61dz3k4ihXlBTgmWJs5NddO4HjpT8FI3z0SQn6aykOMzH
gBpiznj2sgv9iiokzGntqZo0LJdBNJ2997cf7mNIEeMaZXdQhMKQU7XFf9pDTo74U/ygJ7OtXqK1jW
db+OhAY0V0sTTXFSiTSUk2YziL3MFWS1aHlLU5N7I6h9CqyztoiGwn5d/1rbTk3/KdrIlwziYUBZZ9CK
8PCc/oiJIEBD9oDg/CK2H+KkpKChMsXzOv0B9KvsW12iWvgrLhPYHtU+ni7465EVvYPCsYOxev1qQ
qs4B2GVeCxo6kyQLqgjx4wIcGLHx5AgMBAAGjOzA5MAkGA1UdEwQCMAAwCwYDVR0PBAQDAg
GGMB8GA1UdIwQYMBaAFLU1sKRXC/kwcet03DIXvSIfcyhnMA0GCSqGSIb3DQEBCwUAA4IBAQB
FsnoA2UtugIE+kKwY3GdUlKv6bj0oyhbaHFwi8ewR/WI1abdertApefLmk0Aa+5PFya+KaZCWkZlDK
0RlJ1J624yXS+Yh3NnbWOieBKfeax31h6peytMgd85adqxhiEowYTHWJ/PkSku+AFGieMlLtzDIcy/C
Vvs5l4CcHvjLsrhdowwOUIi4v1OS9zKaRgwp/bzhP0ZuDW7JjaqzFIKwwbi+6cs3HLPvTBAGeED5Oe
wFsTxaZnJa0Skqgoi0VQYIurRf50AOG3/bP0Osh6MWylQZRIuNl3A7jxz3sDqsBW+weIq4Qj8A5d97
/7ctQNKe6/PGVpNop3W2dgJS9FUt",
   "mi": "PB400",
   "nmPoints": "46",
   "pCount": "0",
   "pType": "0",
   "qScore": "100",
   "rdsID": "PRECISION.AND.101",
   "rdsVer": "1.1.0",
   "sessionKey":
"M1++JGFa/Vp4szTGOFK0G3NNsVqGo0ffD4xnBf5QZOf8TKO02ap9eWN6ZpTcXrkM+VlyJ0DZkQf
CcrjIcAlh49Mw9a6wcipIJ0lS+wGN6szA1LH85c7Ciem/HNVGW7GH9u21cfSpnEmXlBKtfd5IULTnO
VPF7PfufgFCXC3rSsX8zWOogbEZmKP6eiyw3+gqRb10NyKn90qJGLioBcMaNPt32r5kW2ppne07A
TQLuWZqLdhzVX1tHimCTjm5NchQIAFjrjBKWXVGdEIZ44VJEeeyTa+A6J/Fp4n/8whidnYob+XKQ8/
PvEsu6oSXRwiL1N7QGP8RP48+S57mzIawLw\u003d\u003d"
 },

 "cardnumberORUID": {
   "adhaarNumber": "123443211234",
   "indicatorforUID": 0,
   "nationalBankIdentificationNumber": "607152"
 },
```

```
 "latitude": 13.0641367,
 "longitude": 80.2480973,
 "requestRemarks": "TN3000CA0006530",
 "transactionType": "AUO",
 "merchantUserName": "sai",
 "merchantPin": "81DC9BDB52D04DC20036DBD8313ED055",
 “superMerchantId:”2”,
“merchantTranId”:”13612876AHAS”
“mobileNumber”:”9999999999’
“serviceType”: “AEPS”
}
```


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 for performing the transaction.	**The IIN list can be fetched from (ie, merchant bank details URL** **AEPS-** https://fingpayap.tapits.in/fpaepsservice/api/bankdata/bank/details **Adhaar pay** https://fingpayap.tapits.in/fpaepsservice/api/bankdata/bank/aadharpay

		(M)
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**
transactionType	Type of the transaction	**AUO**
Latitude	Latitude of the place where transaction is happening	**(M)**
Longitude	Longitude of the place where transaction is happening	**(M)**
requestRemarks	If customer or merchant wants to send some remarks	
captureResponse	This response we receive it from the scanner dependent RD SERVICE , 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.**
MerchantTranId	Client reference transaction id to check the transaction status. You must generate a unique merchantTransactionid every time while initiating a transaction.	
Timestamp	Timestamp of the transaction	**(M)**
merchantUserName	Username of the merchant which is registered under Fingpay as a merchant	**(M)**
merchantPin	Pin of the merchant who is onboarded.	**Password must be MD5 hashed(M)**
superMerchantId	Supermerchant id of the company	**(M)which is shared by fingpay**
tefPkId	Reference id for the transaction	**(M)**
fingpayTransactionId	Fingpay generated unique reference id	**(M)**
serviceType	Either AEPS or AP	**(M)**
mobileNumber	Mobile number	**(M)**

RESPONSE PARAMETERS :

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

data :

```
private String fingpayTransactionId;
private Integer tefPkId;
private String bankRrn;
private String fpRrn;
private String stan;
private String merchantTranId;
private String responseCode;
private String responseMessage;
private String mobileNumber;
private String transactionTimestamp;
```

SAMPLE RESPONSE:

```
{
"status": true,
 "message": "Request Completed",
 "data": {
  "tefPkId ": "1234",
  "stan":”123456”,
  "bankRRN":"765765656857" ,
  "fpRrn": "123456",
  "fingpayTransactionId": "XYZ1234",
  "merchantTranId":"123221",
  "responseCode":"00",
  “responseMessage”:”Success”,
  “mobileNumber”:”99897126126’,
  “transactionTimestamp”:”2020-03-09 17:06:00’
 },
 "statusCode": 10000
}
```

Parameter name	Description
tefPkId	Reference number
transactionTimestamp	Requested timestamp
mobileNumber	Mobile number of the BC to which OTP is sent
stan	Reference number of the transaction

bankRRN	Unique id generated by bank which we will receive in the response from bank
fpRrn	Unique reference number generated by Fingpay
fingpayTransactionId	Transaction id generated by Fingpay
merchantTranId	Merchant transaction id sent by client
responseCode	Responsecode
responseMessage	Response message

Checklist for integration:

- Need to perform authentication daily once before doing the transaction for AEPS and Aadhaar pay seperatly
- Should consider the authentication success when the Response code is '00' .
- **If the response code is "FP069" in the transaction response model of all AEPS and AP transcations, aggregator has to initiate the 2FA before doing the transaction.**

Sample response of the transaction API**:**


```
{
 "status": false,
 "message": "Please do 2FA Authentication to initiate transaction",
 "data": {
  "transactionAmount": null,
  "retrievalReferenceNumber": null,
  "responsecode": "FP069",
  "requestedRemarks": null,
  "errorCode": null,
  "errorMessage": null,
 },
 "statusCode": 10030
}
```