Brought to you by ICICI Bank

`

Payment Gateway Integration Document

For

Offline and Online Modes

Dated: 22-Dec-2020

1. Introduction

Eazypay is a first of its kind secure payment service by ICICI Bank in India. It enables institutions to collect money from their customers through multiple payment modes. ICICI Bank is the first and only bank to offer such a payment service in India. The service offers multiple payment modes, both offline and online- like Cash, Cheque, NEFT/RTGS, Cards, Net Banking and UPI. It enables the institution to collect money from any bank customer in India. Offline modes of payment allow the customer to download the payment challan and physically deposit the funds in the bank branch. Online modes allow real time payment by the customer.

The Integration document helps the Payment Gateway Merchants on understanding the payment gateway Integration. This enables the Merchant with Payment option for Offline Payment Modes CASH, Cheque and RTGS/NEFT and Online Modes (Net Banking, Credit Card, Debit Card and UPI)

2. Integration

The web integration / Mobile Integration needs to be initiated with the below section from Process Flow section to the end of the document. The merchant should follow the steps mentioned in the document and use the details shared by ICICI Bank for integration. Before the integration process can begin, the merchant should be enrolled in ICICI Bank as a payment gateway merchant. The merchant ID and encryption key will be shared after the enrollment process is complete.

The Merchant website, web application or mobile application should pass the **referer** parameter in each request in the header of the request. The referer parameter is used to validate the source domain of the PG request. In case the referer parameter is received as null, the request will not be processed and will lead to a session expired error.

Please Note:

- In case the merchant wishes to whitelist the referer, this can be enabled during enrollment. All the requests will be validated in eazypay by the input referer. On authentication the request will be processed, otherwise session expired error will be prompted. **This is only valid for merchants who have opted for dynamic return URL functionality**. In case of a static return URL, domain whitelisting is not required but the referer should be present in the request header to avoid the session expired error. To ensure that the referer is sent automatically in the browser header of the request, the PG request should be initiated using Form Submit.

- Eazypay validates the request from the merchant in the form of referer tag in the browser header. Mobile applications are not able to pass the referer parameter due to technological constraints. To facilitate integration in these cases, the merchant should have an interface hosted web internet application page as payment collection confirmation page. On confirmation the request will be posted to eazypay. Through this approach the merchant can pass the referer in mobile application integration and further process would remain the same.

3. Process Flow

3.1 Merchant Enrollment Flow

- The merchant should be enrolled in eazypay as Category "PG" and should be in the approved state.
- Merchant should share the URL on which the redirection will done after the transaction is completed. This URL is referred to as the return URL and should be configured during enrollment.
- Charges should be configured as per the agreement between the merchant and ICICI Bank.
- The merchant should share the custom configuration including the Mandatory and Optional Fields that need to be configured as per the business needs.
- If the merchant requires the real time MIS for Offline payment modes, this should be opted in during enrollment. The push URL should be shared with ICICI Bank where eazypay will push the real time confirmation in encrypted XML format.
- The push URL will also receive the daily settlement MIS in encrypted XML format if it is configured in eazypay. The settlement MIS is sent once a day through email to the registered email IDs and also sent to the push URL in encrypted XML format.
- Merchant will be registered with the payment modes opted for by their customers. After enrollment, eazypay generates the merchant unique KEY for encryption. This encryption key and the eazypay merchant ID will be shared to the merchant by ICICI Bank
- The merchant can proceed for integration using the merchant ID and encryption key shared by ICICI Bank

3.2 Merchant Integration Flow

- The merchant must check the sample URLs provided in the examples section below. Using this example as a template, the PG request URLs can be generated by replacing the sample data with the merchant specific data and parameters.
- Please check the enrollment PDF sent to the merchant after enrollment is successfully completed. The document contains the custom configuration opted for by the merchant.

- Generate the various URL parameters as per the configuration. Please ensure that the correct data type and size restrictions are adhered to otherwise errors will be prompted.
- After the URL parameters have been generated as per the configuration, encrypt these parameters using the code provided in the document and the AES encryption key provided by ICICI Bank on successful enrollment.
- Once the URL is generated, initiate the payment using form-submit.
- Configure the return URL to read the parameters that are sent in the transaction response. Eazypay will send a response for both successful and failed cases. Response will also be sent in cases where the merchant is not able to land on the payment page. By reading the response in these cases, the merchant can identify the reason for the failure.
- **Static Return URL**: A maximum of 3 return URLs can be configured at the time of enrollment. For static return URL merchants, only send those return URLs in the request which are configured at the time of enrollment. If any other return URLs are sent in the PG request, error will be prompted.
- **Dynamic Return URL:** The dynamic return URL functionality allows the merchant to send any return URL in the PG request and eazypay will redirect to the same after the transaction is completed. Dynamic return URL functionality requires that the source domain of the PG request should be whitelisted before integration can proceed. Please share the list of domains from where the request will be initiated and the ICICI team will whitelist the same during enrollment. In case the request is sent from any domain other than the whitelisted domains, the session will be expired.
- Corporate Internet Banking credentials are required to access the Eazypay dashboard and MIS reports.

3.3 Request Packet Format

The below mentioned parameters have to be sent in the PG request URL after encryption

Parameter Name	Description
merchantid	6 digit Eazypay ICID shared by ICICI Bank
mandatory fields	Mandatory parameters as enrolled in eazypay
optional fields	Optional parameters as enrolled in eazypay

returnurl	Return URL configured while merchant registration in eazypay. Transaction response is sent to this URL.
Reference No	Unique transaction reference no. generated by the merchant's system while initiating eazypay payments
submerchantid	A numeric value that can be customized by the merchant and used to differentiate between internal business units of the merchant (if applicable). In case, internal differentiation is not required, the merchant can send any numeric value less than the maximum size configured for this parameter
transaction amount	Numeric to max limit of 9 digits and decimal two places
paymode	Cash=0,Cheque=1,NEFT/ RTGS=2,NetBanking=3,DebitCard=4,CreditCard=5 and UPI = 6 and All=9 * You Need to send only the number values mapped to the paymode * if any merchant requires to opt for the Debit Card option excluding ICICI Bank Debit Cards, then the pay mode which is specifically enabled for collection should be passed as "8" (paymode = 8)

Note:

- Please append the above parameters with prefix https://eazypay.icicibank.com/EazyPG? (Please see the sample URLs provided).
- Please ensure that the correct encryption key is used for AES encryption.
- Only "transaction amount" in the packet will be considered for the payment process. The transaction amount parameter should be the sum of all the amount fields that are configured in eazypay during enrollment.
- Convenience fees and applicable service tax will be added to the transaction amount as per the agreement between Merchant and ICICI Bank. In case, the charges are borne by the payer, the extra charges will be added to the transaction amount. If the charges are to be

borne by the merchant, the charges will be debited from the merchant's account during settlement.

- The merchant should store the unique reference no generated at their end. This parameter can be used to check the real time status of the transaction in case the transaction response is not received due to network connectivity issues or in case the payer closes the payment page before the redirection to the return URL can take place. Please check the Verify URL section of this document.
- In case of paymode = 8, only non-ICICI Debit Card collections will be enabled. The merchant has an option to display their logo in the payment page. Once the logo is enabled and uploaded, it will be displayed on the payment page otherwise the eazypay logo will be displayed in the same area.

3.4 Examples of Encryption and URL creation

3.4.1 Merchant Configuration (Sample)

Please check the configuration in the eazypay setup PDF shared by ICICI Bank. The below parameters are a sample value. In the below example, there are 3 mandatory fields and 2 optional fields. The sample URLs that are provided below are sample URLs and the merchant should replace their own parameters in the same.

Parameter	Field Type	Field Size	Mandatory
Reference No	String	30	Yes
Sub Merchant Id	String	30	Yes
PGAmount	Amount	9	Yes
Mobile No	Mobile	10	No
Amount2	Amount	9	No

3.4.2 Dummy AES Key for Encryption

Key: 1234567891234567

3.4.3 Before Encryption

https://eazypay.icicibank.com/EazyPG?merchantid=100011&mandatory fields=8001|1234|100&optional fields=9876543212|100&returnurl=https://merchant.url/return.aspx&Reference No=8001&submerchantid=1234&transaction amount=200&paymode=9

3.4.4 After Encryption

https://eazypay.icicibank.com/EazyPG?merchantid=100011&mandatory fields=EDYT659DviojlxZBWK8n0w==&optional fields=7fjcK0w+s8n7P0sVf5DFsQ==&returnurl=XvOMcfrR+gPXMJjzvaMjvOiWN4jXCDY3v4G4fghy/ZhUVd4aE9uYT2Z9B6DaKLB0&Reference No=X7VX+1ZnKq+o6K2QWCTERQ==&submerchantid=QVZkBomDLSbitS4C9lGaUA==&transaction amount=LSMN4y95G1TY0RaXXXbtcQ==&paymode=nFRjDWSCg0m80aUYivDlqw==

In the above sample URL, please note the following:

- Mandatory and optional fields are separated using the "|" character. In case the merchant is not sending specific optional fields, the blank fields should be replaced by a space. eg. In case there are 4 optional fields and the merchant is not sending the 1st, 3rd and 4th field, then the optional fields should be configured as " |sample| | "
- There are 2 amount fields with Rs. 100 as the amount in both the fields. Therefore the total amount in the "transaction amount" parameter is the sum of both the amounts : Rs. 200
- Sub-merchant ID is a numeric value

Before merchant moves to production for real time transactions, please ensure the following:

- Encrypt the plain text data with AES Key shared above for the purpose of testing. Please use the code provided in the document as per your technological framework.
- After encryption, the data should match the same with the encrypted data in the sample URL.
- Replace the above parameters with your own merchant specific parameters (as per merchant configuration) and then encrypt the same with the AES Key shared by ICICI Bank.

3.5 Response Packet Parameters

These parameters will be sent to the merchant as soon as the transaction has been completed and eazypay redirects to the registered merchant's return URL sent in the PG request. The below mentioned parameter names can be used to read the response data.

#	Parameters	Description	Type	Min	Max	Deci-mals	Mandatory	e.g Data
1	Response Code	Section 4	Char	3	6		Yes	As per error codes mentioned in the Error Codes Table e.g E000
2	Unique Ref Number	A Unique Trans-action ID gener-ated by eazypay	Nu-meric	16	16		Yes	Eazypay tran id e.g 1234567891234
3	Service Tax	Service Tax	Nu-	1	6	2	Yes	1.00

#	Parameters	Description	Type	Min	Max	Decimals	Mandatory	e.g Data
	Amount	amount on the transaction amount	meric					
4	Processing Fee Amount	Convenience amount on the transaction amount	Numeric	1	6	2	Yes	1.00
5	Total Amount	Transaction Amount with convenience fee and service Tax	Numeric	1	9	2	Yes	10.00
6	Transaction Amount	Transaction Amount as received from the PG Merchant	Numeric	1	9	2	Yes	8.00
7	Transaction Date	Transaction Date and Time in Response from eazypay	Date				Yes	03-05-2016 17:18:32
8	Interchange Value	Interchange Value	Numeric	1	3	0	Yes	Blank
9	TDR	TDR	Numeric	1	3	0	Yes	Blank
10	Payment Mode	Opted by the Payer for a Transaction	Char	4	20		Yes	<Opted payment mode> e.g. NET_BANKING
11	SubMerchantId	Sub Merchant ID as shared in Request Packet	Char	1	30		Yes	1234
12	ReferenceNo	Reference No shared by the	Char	1	30		Yes	8001

#	Parameters	Description	Type	Min	Max	Decimals	Mandatory	e.g Data
		Merchant in Request Packet						
13	TPS	Third Party Status	Char	1	30		Yes	Null for CASH, CHEQUE, NEFT/RTGS 0 (zero) for Net Banking Credit Card, Debit Card
14	ID	Merchant eazypay ID	Numeric	6	6		Yes	100011
15	RS	SHA1 512Signature	ID|Response Code|Unique Ref Number|Service Tax Amount|Processing Fee Amount|Total Amount|Transaction Amount|Transaction Date|Interchange Value|TDR|Payment Mode|SubMerchantId|ReferenceNo|TPS|aes_key				Yes	100011|E000|1234567891234|1.00|1.00|10.00|8.0|03-05-2016 17:18:32|||NET_BANKING|1234|8001|null|1234567891234567

Note:

- All the above response parameters will be in Plain text.
- On receipt of response from eazypay to the merchant website, generate the SHA512 Signature after receipt of response and match SHA512 Signature received in the response in parameter "RS".
- On receiving the response, generate the SHA512 signature using the response parameters. Match the generated value with the value received in the "RS" parameter. If the values match, then the response should be considered as valid.
- If the SHA512 signature generated by the merchant and the one received in the response does not match, reject the response packet and inform ICICI Bank.

4. Error Handling

Errors will be prompted by eazypay for multiple cases where the request parameters are not correct or the transaction has failed. All the cases where errors can be encountered will be sent to the merchant's return URL in the "Response Code" parameter. The merchant can read this parameter and refer the table below to find out the error reason.

In case, the Response Code is "E000", the transaction should be considered as success for all online payment modes. In case of offline payment modes like Cash, Cheque and NEFT/RTGS, the merchant will receive a response once the challan has been generated. If real time MIS push has been opted in by the merchant during enrollment, a real time notification will sent when the funds are received successfully against the challan.

The list of Error Codes is given below:

Error Code	Description
E000	Received successful confirmation in real time for the transaction. Settlement process is initiated for the transaction.
E001	Unauthorized Payment Mode
E002	Unauthorized Key
E003	Unauthorized Packet
E004	Unauthorized Merchant
E005	Unauthorized Return URL
E006	Transaction is already paid
E007	Transaction Failed
E008	Failure from Third Party due to Technical Error
E009	Bill Already Expired
E0031	Mandatory fields coming from merchant are empty
E0032	Mandatory fields coming from database are empty
E0033	Payment mode coming from merchant is empty

E0034	PG Reference number coming from merchant is empty
E0035	Sub merchant id coming from merchant is empty
E0036	Transaction amount coming from merchant is empty
E0037	Payment mode coming from merchant is other than 0 to 9
E0038	Transaction amount coming from merchant is more than 9 digit length
E0039	Mandatory value Email in wrong format
E00310	Mandatory value mobile number in wrong format
E00311	Mandatory value amount in wrong format
E00312	Mandatory value Pan card in wrong format
E00313	Mandatory value Date in wrong format
E00314	Mandatory value String in wrong format
E00315	Optional value Email in wrong format
E00316	Optional value mobile number in wrong format
E00317	Optional value amount in wrong format
E00318	Optional value pan card number in wrong format
E00319	Optional value date in wrong format
E00320	Optional value string in wrong format
E00321	Request packet mandatory columns is not equal to mandatory columns set in enrolment or optional columns are not equal to optional columns length set in enrolment
E00322	Reference Number Blank
E00323	Mandatory Columns are Blank
E00324	Merchant Reference Number and Mandatory Columns are Blank
E00325	Merchant Reference Number Duplicate
E00326	Sub merchant id coming from merchant is non numeric
E00327	Cash Challan Generated

E00328	Cheque Challan Generated
E00329	NEFT Challan Generated
E00330	Transaction Amount and Mandatory Transaction Amount mismatch in Request URL
E00331	UPI Transaction Initiated Please Accept or Reject the Transaction
E00332	Challan Already Generated, Please re-initiate with unique reference number
E00333	Referer is null/invalid Referer
E00334	Mandatory Parameters Reference No and Request Reference No parameter values are not matched
E00335	Transaction Cancelled By User
E0801	FAIL
E0802	User Dropped
E0803	Canceled by user
E0804	User Request arrived but card brand not supported
E0805	Checkout page rendered Card function not supported
E0806	Forwarded / Exceeds withdrawal amount limit
E0807	PG Fwd Fail / Issuer Authentication Server failure
E0808	Session expiry / Failed Initiate Check, Card BIN not present
E0809	Reversed / Expired Card
E0810	Unable to Authorize
E0811	Invalid Response Code or Guide received from Issuer
E0812	Do not honor
E0813	Invalid transaction
E0814	Not Matched with the entered amount
E0815	Not sufficient funds
E0816	No Match with the card number

E0817	General Error
E0818	Suspected fraud
E0819	User Inactive
E0820	ECI 1 and ECI6 Error for Debit Cards and Credit Cards
E0821	ECI 7 for Debit Cards and Credit Cards
E0822	System error. Could not process transaction
E0823	Invalid 3D Secure values
E0824	Bad Track Data
E0825	Transaction not permitted to cardholder
E0826	Rupay timeout from issuing bank
E0827	OCEAN for Debit Cards and Credit Cards
E0828	E-commerce decline
E0829	This transaction is already in process or already processed
E0830	Issuer or switch is inoperative
E0831	Exceeds withdrawal frequency limit
E0832	Restricted card
E0833	Lost card
E0834	Communication Error with NPCI
E0835	The order already exists in the database
E0836	General Error Rejected by NPCI
E0837	Invalid credit card number
E0838	Invalid amount
E0839	Duplicate Data Posted
E0840	Format error

E0841	SYSTEM ERROR
E0842	Invalid expiration date
E0843	Session expired for this transaction
E0844	FRAUD - Purchase limit exceeded
E0845	Verification decline
E0846	Compliance error code for issuer
E0847	Caught ERROR of type:[System.Xml.XmlException] . strXML is not a valid XML string Failed in Authorize - I
E0848	Incorrect personal identification number
E0849	Stolen card
E0850	Transaction timed out, please retry
E0851	Failed in Authorization - PE
E0852	Cardholder did not return from Rupay
E0853	Missing Mandatory Field(s)The field card_number has exceeded the maximum length of 19
E0854	Exception in CheckEnrollmentStatus: Data at the root level is invalid. Line 1, position 1.
E0855	CAF status = 0 or 9
E0856	412
E0857	Allowable number of PIN tries exceeded
E0858	No such issuer
E0859	Invalid Data Posted
E0860	PREVIOUSLY AUTHORIZED
E0861	Cardholder did not return from ACS
E0862	Duplicate transmission
E0863	Wrong transaction state

E0864	Card acceptor contact acquirer

5. Online Refund Service

This service will facilitate the refund for settled transactions from the merchant's account to the payer's account. Once the transaction is initiated for refund, the eazypay operations team will approve/reject the same. On approval from the eazypay operations Team, the merchant account will be debited and the payer account will be credited.

5.1 Process Flow Prerequisites and Details

- Merchant should have opted for the refund service with eazypay.
- Refunds can only be initiated for successful and settled transactions.
- In order to access the Refund Service, merchant's IP from where the request is initiated should be white-listed by eazypay. Only white-listed IPs requests will be responded to by eazypay and therefore, the merchant must ensure that the request is only sent from the whitelisted IPs
- After the IPs are white-listed, ICICI bank will share a unique private key. This key must be sent in the request header for each refund request. This header key is used to validate the source IP of the request.
- Merchant initiates the refund request with respective request parameters and eazypay refund service initiates the refund and sends a response back to merchant with response parameters.
- If the refund request is successful, a success response will be sent to the merchant and in case of failure, the response will contain a message describing the error.
- For each successful refund request, eazypay initiates the refund and passes the refund request to the Eazypay operations team. The team then debits the merchant's account and credits the payer's account as per the process.

5.2 Request and Response parameter details

Request Parameters

Parameter Name	Description	Type	Min	Max	Mandatory	Example
MerchantId	Eazypay Merchant ID (as provided by ICICI Bank at the time of enrollment	String	6	8	Yes	107486
inputdata	Encryption of JSON data with AES Key (as provided by ICICI Bank at the time of enrollment)	String			Yes	JSON Parameters from below table

Create a JSON packet using the parameters in the below table and then encrypt the entire packet using the AES encryption key provided by ICICI Bank.

Parameter Name	Description	Type	Min	Max	Mandatory	Example
Paymode	Payment Mode (List of payment modes is provided in a table below)	String	10	25	Yes	NET_BANKING
TransactionID	Eazypay Transaction ID (received in the transaction response)	String	13	16	Yes	17081815917276
Transaction-Date	Date of initiation of transaction	String	10	10	Yes	2019-08-18 (YYYY-MM-DD)
MerchantId	Eazypay Merchant ID (as provided by ICICI Bank at the time of enrollment	String	6	8	Yes	107486
UserId	A parameter that can be used as a	String	1	8	Yes	Merchant specific parameter like User Name, Refer-

Parameter Name	Description	Type	Min	Max	Mandatory	Example
	refund reference no, user name, Unique ID. This parameter is not validated at eazy-pay's end.					ence Number, Unique ID etc.
Refun-dAmount	Amount that is to be refunded.	String	1	8	Yes	10
signature	SHA 512 signature hash value. Gener-ated using the plain string : merchantId|trans-actionID|refun-dAmount	String			Yes	a7688c1843fe28c90599949 c64935d3bbf36ee216e6353 41ec8a42850a02b2950c45c 66b9069ad82d92e-b92aa4428010d9400cd599 0a1881111d97aa8e000617

Response Parameters

The below parameters will be received as soon as the request has been processed by eazypay

Response Parame-ter	Description	Type	Min	Max	Mandatory	Example
Status	Status of the Refund Re-quest	String	1	1	Yes	Y for Success N for Failed
Message	Message de-scribing the success/failure cases	String			Yes	Refund Initiated Suc-cessfully.
Total Refunded Amount	Total Refunded Amount	Numeric	1	7	Yes	10
TransactionID	TransactionID	Numeric	12	15	Yes	20011415917513
ErrorMessage	ErrorMessage	String	1	15	Yes	SUCCESS
signature	SHA 512 signa-ture hash	String			Yes	a7688c1843fe28c9059 9949c64935d3bbf36ee

Response Parameter	Description	Type	Min	Max	Mandatory	Example
	value. Generated using the plain string : Status|Message|ErrorMessage					216e635341ec8a42850a02b2950c45c66b9069ad82d92e-b92aa4428010d9400cd5990a1881111d97aa8e000617

5.3 Steps for Online Refund Service

- IPs must be be whitelisted before the service can be launched, Please contact ICICI Bank and the respective team will do the needful.
- Create the JSON packet using the parameters provided in the request packet table, The keys for the key and value pairs are mentioned in the table and values must be as per the size and data types mentioned in the same table.
- Encrypt the entire JSON packet for the inputdata parameters using the encryption key provided by ICICI Bank at the time of enrollment. This value will be the value of inputdata for the final JSON packet.
- Using the merchant ID provided by ICICI Bank after enrollment and the above mentioned encrypted value create the final JSON packet.
- Enter the private_key in the request header. This value is provided by ICICI Bank after IPs have been whitelisted.
- In the request body, the final JSON packet should be present.
- Send the request to the URLs that are mentioned below using the POST method.
- Eazypay will send a response immediately after the rewuest has been processed. The response will contain a message specifying whether the refund has been initiated successfully or not. The list of parameters in the refund API response are mentioned in a table below.

- Once eazypay has successfully initiated the refund, as per process the merchant's account is debited and the payer's account is credited with the funds.
- The merchant can check the real time status of the refund request and the preceeding history of refunds for a particular transaction using the Refund History MIS Service which is mentioned in this document.
- Multiple partial refunds are allowed in eazypay as long as the Total Refunded Amount is not greater than the Transaction Amount.

5.4 List of Payment Modes for the Paymode parameter:

Payment Mode	Value to be sent in paymode parameter
Cash	CASH
Cheque	CHEQUE
RTGS and NEFT	NEFT_RTGS
Netbanking (ICICI Bank)	NET_BANKING_ICICI
Netbanking (Other Banks)	NET_BANKING
Debit Card	DEBIT_CARD
Credit Card	CREDIT_CARD
UPI	UPI_ICICI

5.5 URL and Sample Request and Response

Production

https://eazypay.icicibank.com/OnlineRefundService/rest/OnlineRefundService/OnlineRefundDetails

UAT

https://eazypayuat.icicibank.com/OnlineRefundService/rest/OnlineRefundService/OnlineRefundDetails

Request Packet Header

Key : private_key

Value : **BES0EP0AGG** (This is a sample value. Please use the value share by ICICI Bank)

Sample Request Packet:

{"MerchantId":"110301","inputdata":"jfcissO00zyGM2Li8Kc/
Q9SxA5B9wJP1foVLRC2HyPi5lE4JmAIA4FSxr099q5Ul6CwO8E6cANePDqAmrwpm4r4uwB3XL4ux
xZCaFi6QlsXJiTpO3o2ERRvlJCb29SWkuGWkVIPfRqiEAsrAW59VM8VdleWBSPuQadXSh1pa/
+r9/9x/aMMAXr8iYWnQZPM8yC1BlKzS1BxkrSTaUcV92kG10/
aYOYfG2StpK7enOaLoj+Q8A3N7zjWZMbrilBlHPL+uV7MJZWPHt2uZTSDlgHz0aw7iYEPy/
xv3lPBobOFj9FM2Pv1G0GmsrnPT4FS5EUvlQ3/sn/QnLmbFyetC+P/
Urf1Q54EMtMavgXB0JGz2Wly0NiZWTKtiF7lhhxDkpFP9VoOshwg40GACp9Dl7w=="}

Parameters for inputdata

Encrypt the below packet using the encryption key :

{"Paymode":"NET_BANKING","TransactionID":"17091415917513","TransactionDate":"2017-09-
14","MerchantId":"110301","UserId":"PRATEEK",
"signature":"0927d1bbc490e58b6fee8f1a354fedc2c5ee72c70e1232ef60d32f50aee59dc94f4b7a8e9b
fa88701f4fe5d882bab9abd8f94736d38fa884fe0613e911ef9770","RefundAmount":"1"}

Response Packet:

{
"Status": "Y",
"Message": "Refund Initiated Succesfully.",
"Total Refunded Amount": 2,
"TransactionID": "17091415917513",
"ErrorMessage": "",
"signature":

"12e95baad8c6b4879c429401808a162340d1747b33982e458ee1543a8a6c431c1091ef219d55cf4890
1f5ae7420a0884a25d44503874feb68a78a56fd0bdfd0f"}

6. Push Service: Real Time Transaction Notification Service

Eazypay will provide a real time transaction notification to the merchant on receipt of confirmation from the source banks to eazypay for applicable payment modes.

This service notification confirmation ensures that the merchant receives real time status for all the transactions. Real time confirmation will be provided in encrypted XML format which can be decrypted using the AES Key shared by ICICI Bank during enrollment. The service notification will be sent on the merchant's registered Push URL.

Both real time transaction notification and EOD MIS push will be sent on the same Push URL. The merchant needs to read the packets differently using the identifier tags and configure their system accordingly.

To enable the service, the respective applicable parameters should be configured in the offline enrollment portal in the **Configuration details tab → Online/Offline Details → EOD MIS Push (XML) "Yes" → Enable "YES" in Real Time Notification option** (by default it will be disabled as "No"). On selecting this option, the URL on which the real time transaction notification will be pushed has to be specified.

While enabling this, the EOD MIS push URL can be set as either "Yes" or "No". In case No is selected, the EOD MIS will not be shared by eazypay.

Prerequisites for Push Service: Real Time Transaction Notification Service

- Merchant Service will read the string from the URL.
- The string will be encrypted using the AES key mapped to the merchant.
- The merchant should store the Eazypay Merchant ID, AES Key, Account Number etc. for facilitating the reading of the XML packet sent by eazypay.
- Read the XML tags as mentioned in the below table.
- Generate the Hash value (SHA512) with defined parameters at the merchant's end after reading the parameters from the XML data. Match the Hash value generated at the merchant end and received from eazypay. If both values match, then the merchant should consider the data as valid.

XML Packet Details

Request Parameter	Description	Type	Min	Max	Mandatory	Example
RT	Static value for Real Time	String	-	-	Yes	Tran
IcId	Eazypay Merchant ID	String	6	8	Yes	107486
TrnId	Eazypay Tran ID	String	13	15	Yes	17091915917603
PayMode	Payment Mode	String	4	20	Yes	CHEQUE, CASH, DEBIT_CARD etc.
TrnDate	Transaction Date	String	10	10	Yes	2017-09-19 14:39:35.0
SettleDT	Settlement Date	String	10	10	Yes	NA
Status	Transaction Status	String	5	15	Yes	Success
ResponseCode	Response Code as described in Section-4	String	3	6	Yes	As per error codes mentioned in the Error Codes Table e.g E000
InitiateDT	Initiated On	String	10	10	Yes	11-Aug-17
TranAmt	Amount + Taxes	String	1	10	Yes	12
BaseAmt	Amount	String	1	10	Yes	11
ProcFees	Processing Fee	String	1	10	Yes	0.22
STax	S Tax	String	1	10	Yes	0.03
M_SGST	SGST	String	1	10	Yes	0
M_CGST	CGST	String	1	10	Yes	0
M_UTGST	UTGST	String	1	10	Yes	0
M_STCESS	STCESS	String	1	10	Yes	0
M_CTCESS	CTCESS	String	1	10	Yes	0
M_IGST	IGST	String	1	10	Yes	0
GSTState	GST STATE	String	2	4	Yes	MH
BillingState	GST STATE	String	2	4	Yes	MH
Remarks	Remarks	String	1	100	Yes	Subject to Realization
HashVal	SHA512	String			Yes	IcId|TrnId|PayMode|TrnDate|SettleDT|Status|InitiateDT|TranAmt|BaseAmt|ProcFees|STax|

Request Parameter	Description	Type	Min	Max	Mandatory	Example
						M_SGST|M_CGST|M_UTGST|M_STCESS|M_CTCESS|M_IGST|GSTState|BillingState|yyyddmm Example 110451|17091915917603|CHEQUE|2017-09-19 14:39:35.0|NA|Success|03-Oct-17|3678|3628|36.97|0|0|0|0|0|0|7.03|UTCL|JK|20170310

Sample XML packets

<XML><RT>Tran</RT><IcId>131390</IcId><TrnId>20020763351795</TrnId><PayMode>NET_BANKING_ICICI</PayMode><TrnDate>2020-02-07 12:29:21.0</TrnDate><SettleDT>NA</SettleDT><Status>Success</Status><ResponseCode>E000</ResponseCode><InitiateDT>07-Feb-20</InitiateDT><TranAmt>1</TranAmt><BaseAmt>1.0</BaseAmt><ProcFees>0.00</ProcFees><STax>0.0</STax><M_SGST>0</M_SGST><M_CGST>0</M_CGST><M_UTGST>0</M_UTGST><M_STCESS>0</M_STCESS><M_CTCESS>0</M_CTCESS><M_IGST>0.15</M_IGST><GSTState>DL</GSTState><BillingState>MH</BillingState><Remarks>Subject to realization</Remarks><HashVal>878c26cb621799f43b7cae344f15d3085dfa6112f50db14a102c39f2a2c3efbf3549603826d52216aa7766f1823efef64272b10a4843d9ec9b6c2fa69316092c</HashVal></XML>

After Encryption

kZVTJPemp8E787Uexdwkn4iceHn0uPw0Rup7IswupnQCF4bakf47bfCqBHaFWqbRWhH3FO3paMk
a4t9ez1p+gGLChgofcP6iPAmgGTeCzEunqKqNZCstqlfRPB5P4bU2Vy7fv88m+IFuv635Om6OWU1
N qRAK4Gz15tjaWPFY/t3YOtOOqXatB80TxqUqk0w2OgnG0l6TMHUuW/N9fDohY4v9grbn9o0UsTo
YXcej4z/cgLdgLYybuExyrjiqzeXHeK/KREvPaV9L7hBiVpvmHXi0dopFjatM37D3TAMvg63lPeg
tRLaCCFW7Tt+KxxL2QBoM+42NeWduLiJRCCCj8Ax1jqT0EwrQ2EAn1C5wm1sliUiMeuiGOX1M3P
P RR2S8TD8MlTyAszUTMK4EX69EYTyFTdxHS32sm4TscyCDrLUd/xWc8/Da6tl0fksEuklJlJTK84P
YQyhFujrDluY1l/aEDHKs2KDD5D97LlSFo9vs3WNoYQaqlCHP5h0TVW/O4VGtlhhX0pQYtGHKdGr
2Ad3ro1x0ykv37Kp7mpxvlRYtWe06o/uYykkee2F/8sjn++T+eh/l2rLiiAvjWMdRut4N/ZLfljl
pcowkVtwkEN+kz7jglv1HlKgl/LRS5FwWjMJ9r3Lwnxm2rz6up2glO8YhK9Jcdpz5Q8PTfCf3v+f
1JQOZwoiZkrKrBe3FSPuTp5N42CS0cgdZZLG4UnaCxpzeopaAbq1u+exR5HwwNJoWcxNhs8kD9s
Q wTGhzAETlPrcuhNlvt05wDO1V1TKBC/ZWuScGd5xsba/v5YGf4R/2G/l7tXPy5t3TGpkXnR+KkMp
9EbRug==

Decryption Logic: sample code for Java

```
import java.security.Key;
import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;
import sun.misc.BASE64Decoder;
public String decryptFile(String key, String inputParam)
{
byte[] raw = key.getBytes();
SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");
Key secretKey = skeySpec;
Cipher aesCipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
aesCipher.init(2, secretKey);
byte[] plaintext = (byte[])null;
BASE64Decoder encoder = new BASE64Decoder();
byte[] base64 = encoder.decodeBuffer(inputParam);
plaintext = aesCipher.doFinal(base64);
String decf1 = new String(plaintext);
return decf1;
}
```

7. Refund Status Check Service

This service can be used by the merchant to get the current status of refunds that have been initiated through the Online Refund Service.

Steps for the refund status inquiry:

- In order to access the service, merchant's IP from where the request is initiated should be white-listed by eazypay. Only white-listed IPs requests will be responded to by eazypay and therefore, the merchant must ensure that the request is only sent from the whitelisted IPs
- After the IPs are white-listed, ICICI bank will share a unique private key. This key must be sent in the request header for each refund request. This header key is used to validate the source IP of the request.
- Only approved merchants can initiate this service.
- Create a JSON Packet with the parameters mentioned in the request packet for encryptedData.
- After Successful Creation of JSON Packet, encrypt the JSON Packet with Merchant AES Key shared by eazypay.
- Encrypt the entire JSON Map the encryption to the request packet parameter encryptedData as mentioned below and create the final JSON packet.
- Pass the correct header key (as shared by eazypay after IP whitelisting) in the request header.

Request Packet Details:

Request Parameter	Description	Type	Min	Max	Mandatory	Example
merchantId	Eazypay Merchant ID	String	6	8	Yes	123456
encryptedData	Encrypted with AES KEY Allocated to Merchant	String		500	Yes	mvSAcuZIR8H/RmDdDd4UIPv0+Rh8BvC2PnUJXZIFN/1iSyQx+Jrk1Rmu2uju76HMN4Di9mse8AQsbAMkGoomnpEv0q0MNdauZouS4F

						BusLstOedQ8Wv4TCIxpZQtcXRZ+DYk WGfCunGHCJPuAGrImdpJSDxmSd6Yz U4vGLo1laRzoKAt0nd+JlErNVKQji5nlPE D7vjoGJ57sXo9mpo4DGBXq14SaxHGX iSDJnDTaV4gOkV4qhYlzYElsIVR1RDw2 3/hJmbi7yD0J/4F2TjA==

The encryption of encrypted data should be in sequence of data as follows

Request Parameters for encryptedData	Description	Type	Mandatory	Example
transactionId	Eazypay Transaction ID	String	Yes	17102315917912
merchantId	Eazypay Merchant ID as shared by ICICI Bank	String	Yes	103245
signature	SHA512 signature Generated from string: merchantId +"|"+transactionId	String	Yes	284eb6946a30cc1216023f55b2d6b9b8e585e546bb910aad9288504b86d0b4bce4ce7105207dfb9ac6449fb6b86c70fdd449e6b4023947c7a5e104b880d05d55

Response Packet Details

Response Parameters	Description	Type	Example
merchantId	Eazypay transaction ID	String	19061951719627
Refund History	Details of each step of the refund process. Multiple partial refunds will be displayed with the current process status for each.	String	{"processStatus": "Maker Initiated", "refundTransactionStatus": "Initiated", "refundReason": "Success", "paymode": "DEBIT_CARD", "transactionAmount": "13", "uploadStatus": "System_Rejected", "accountNumber": "05540388941105", "transactionDate": "2016-09-08 00:00:00.0", "refundDate": "2017-03-08 10:37:57.0", "baseAmount": "13", "refundAmount": "2" }
Transaction ID	Eazypay Transaction ID	String	1809081556946

URLs and Sample Request and Response Packets:

Production:

https://eazypay.icicibank.com/RefundMISApiService/getRefundDetails

UAT:

https://eazypayuat.icicibank.com/RefundMISApiService/getRefundDetails

Sample Request and Response:

Request Header:

Add the key in Request header in the request packet private_key BES0EP0AGG (case sensitive) as shared by ICICI Bank

Key: private_key

Value: BES0EP0AGG (This is a sample value, please use the value shared by ICICI Bank)

Request:

{"merchantId":"107018","encryptedData":"mvSAcuZlR8H/RmDdDd4UlPv0+Rh8BvC2PnUJXZlFN/1iSyQx+Jrk1Rmu2uju76HMN4Di9mse8AQsbAMkGoomnpEv0q0MNdauZouS4FBusLstOedQ8Wv4TClxpZQtcXRZ+DYkWGfCunGHCJPuAGrlmdpJSDxmSd6YzU4vGLo1laRzoKAt0nd+JlErNVKQji5nlPED7vjoGJ57sXo9mpo4DGBXq14SaxHGXiSDJnDTaV4gOkV4qhYlzYElslVR1RDw23/hJmbi7yD0J/4F2TjA==="}

Plain text encryptedData parameters:

{"transactionId":"1609081556946",

"merchantId":"107018",

"signature":"284eb6946a30cc1216023f55b2d6b9b8e585e546bb910aad9288504b86d0b4bce4ce7105207dfb9ac6449fb6b86c70fdd449e6b4023947c7a5e104b880d05d55"}

Response:

{

"merchantId": "107018",
"Refund History:": [

{

"processStatus": "Maker Initiated",
"refundTransactionStatus": "Initiated",
"refundReason": "Refund amount greater than transaction amount",
"paymode": "NET_BANKING",
"transactionAmount": "13.13",
"uploadStatus": "System_Rejected",
"accountNumber": "05540388941105",
"transactionDate": "2016-09-08 00:00:00.0",
"refundDate": "2017-03-08 10:34:23.0",
"baseAmount": "13",
"refundAmount": "13.13"
},
{
"processStatus": "Maker Initiated",
"refundTransactionStatus": "Initiated",
"refundReason": "Success",
"paymode": "DEBIT_CARD",
"transactionAmount": "13",

```
        "uploadStatus": "System_Rejected",
        "accountNumber": "05540388941105",
        "transactionDate": "2016-09-08 00:00:00.0",
        "refundDate": "2017-03-08 10:37:57.0",
        "baseAmount": "13",
        "refundAmount": "2"
      }
],
   "Transaction ID": "1609081556946"
}
```


7.1 Reports for Reconciliation

The reports can be downloaded from the Corporate Internet Banking for last 90 days transactions in CSV format. Various reports are available for download in CIB.

7.2 Source Code Encryption Functions for Java / .net and PHP

7.2.1 Java Source Code

```
public encryptFile(String key, String inputParam)
{
byte[] abyte2 = (byte[])null;
byte[] abyte1 = key.getBytes();
SecretKeySpec secretkeyspec = new SecretKeySpec(abyte1, "AES");
SecretKeySpec secretkeyspec1 = secretkeyspec;
Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
cipher.init(1, secretkeyspec1);
abyte2 = cipher.doFinal(inputParam.getBytes());
BASE64Encoder encoder = new BASE64Encoder();
String ur_enc_str = encoder.encode(abyte2);
}
```

7.2.2 .Net c#Source Code

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Security.Cryptography;
using System.Text;
using System.Threading.Tasks;

namespace encryptDecrypt
{
   public class EncryptDecrypt
   {
      public static string encryptFile(string textToEncrypt, string key)
      {
         RijndaelManaged rijndaelCipher = new RijndaelManaged();
```

```
        rijndaelCipher.Mode = CipherMode.ECB;
        rijndaelCipher.Padding = PaddingMode.PKCS7;
        rijndaelCipher.KeySize = 0x80;
        rijndaelCipher.BlockSize = 0x80;
        byte[] pwdBytes = Encoding.UTF8.GetBytes(key);
        byte[] keyBytes = new byte[0x10];
        int len = pwdBytes.Length;
        if (len > keyBytes.Length)
        {
           len = keyBytes.Length;
        }
        Array.Copy(pwdBytes, keyBytes, len);
        rijndaelCipher.Key = keyBytes;
        rijndaelCipher.IV = keyBytes;
        ICryptoTransform transform = rijndaelCipher.CreateEncryptor();
        byte[] plainText = Encoding.UTF8.GetBytes(textToEncrypt);
             return Convert.ToBase64String(transform.TransformFinalBlock(plainText, 0, plainTex-
t.Length));
      }
   }
}
```

7.2.3 .Net VB Source Code

```
Imports System.Collections.Generic

Imports System.IO

Imports System.Linq

Imports System.Security.Cryptography

Imports System.Text

Imports System.Threading.Tasks

Namespace encryptDecrypt

        Public Class EncryptDecrypt
```

```
        Public Shared Function encryptFile(textToEncrypt As String, key As String) As
String
                Dim rijndaelCipher As New RijndaelManaged()
                rijndaelCipher.Mode = CipherMode.ECB
                rijndaelCipher.Padding = PaddingMode.PKCS7
                rijndaelCipher.KeySize = &H80
                rijndaelCipher.BlockSize = &H80
                Dim pwdBytes As Byte() = Encoding.UTF8.GetBytes(key)
                Dim keyBytes As Byte() = New Byte(15) {}
                Dim len As Integer = pwdBytes.Length
                If len > keyBytes.Length Then
                        len = keyBytes.Length
                End If
                Array.Copy(pwdBytes, keyBytes, len)
                rijndaelCipher.Key = keyBytes
                rijndaelCipher.IV = keyBytes
                Dim transform As ICryptoTransform = rijndaelCipher.CreateEncryptor()
                Dim plainText As Byte() = Encoding.UTF8.GetBytes(textToEncrypt)
                Return    Convert.ToBase64String(transform.TransformFinalBlock(plain-
Text, 0, plainText.Length))
        End Function
    End Class
End Namespace
```

7.2.4 PHP Source Code

```
function aes128Encrypt($str,$key){
$block = mcrypt_get_block_size('rijndael_128', 'ecb');
$pad = $block - (strlen($str) % $block);
$str .= str_repeat(chr($pad), $pad);
```

return base64_encode(mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key, $str, MCRYPT_MODE_ECB));

}

7.3 SHA 512 Signature

7.3.1 .Net C# Source Code

```
using Microsoft.VisualBasic;
using System;
using System.Collections;
using System.Collections.Generic;
using System.Data;
using System.Diagnostics;
using System.Text;
using System.Security.Cryptography;
namespace CodeShare.Cryptography
{
	public class SHA
	{
		public static string GenerateSHA512String(inputString)
		{
			SHA512 sha512 = SHA512Managed.Create();
			byte[] bytes = Encoding.UTF8.GetBytes(inputString);
			byte[] hash = sha512.ComputeHash(bytes);
			StringBuilder stringBuilder = new StringBuilder();
			for (int i = 0; i <= hash.Length - 1; i++) {
				stringBuilder.Append(hash(i).ToString("x2"));
			}
			return stringBuilder.ToString();
		}
	}
}
```

7.3.2 .Net VB Source Code

```
Imports System.Text
Imports System.Security.Cryptography
Namespace CodeShare.Cryptography
Public Class SHA
Public Shared Function GenerateSHA512String(ByVal inputString) As String
    Dim sha512 As SHA512 = SHA512Managed.Create()
    Dim bytes As Byte() = Encoding.UTF8.GetBytes(inputString)
    Dim hash As Byte() = sha512.ComputeHash(bytes)
    Dim stringBuilder As New StringBuilder()
    For i As Integer = 0 To hash.Length - 1
      stringBuilder.Append(hash(i).ToString("x2"))
    Next
    Return stringBuilder.ToString()
  End Function
 End Class
End Namespace
```

7.3.3 JAVA Source Code

```
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
public class SHA512Signature {
   public static void main(String[] args) {
                String   hashString1="100011|E000|1234567891234|1.00|1.00|10.00|8.0|03-05-2016
17:18:32|||NET_BANKING|1234|8001|null|1234567891234567";
      String hashSignature = new SHA512Signature().hashCal("SHA-512",hashString1);  }
   public String hashCal(String type,String str){
      byte[] hashseq=str.getBytes();
      StringBuffer hexString = new StringBuffer();
      try{
      MessageDigest algorithm = MessageDigest.getInstance(type);
```

```
    algorithm.reset();
    algorithm.update(hashseq);
    byte messageDigest[] = algorithm.digest();
    for (int i=0;i<messageDigest.length;i++) {
       String hex=Integer.toHexString(0xFF & messageDigest[i]);
       if(hex.length()==1) hexString.append("0");
       hexString.append(hex);       }
    }catch(NoSuchAlgorithmException nsae){ }
    return hexString.toString();    }
}
```

7.4 Assumptions and Dependencies

- All request parameters should be encrypted, AES encryption key will be shared by the sales team to the merchant after successful enrollment.
- All payment modes enrolled by the merchant will be displayed on the payment page if paymode parameter is sent as "9"
- Payer can re-initiate the transaction from the payment gateway, in case of any error.
- Merchant should be in approved state before integration can begin.
- Once Merchant is registered as PG, then change to any other category is not allowed.
- For successful transactions, only the transaction amount will be settled to the merchant.
- The Transaction journey can be validated from MIS Reports, or transaction enquiry through CIB Module. Real time transaction status can be checked using the Verify URL.
- After eazypay receives confirmation from the bank, the transaction will undergo the journey as follows :

  Receipt Confirmation from Bank ☾ Reconciliation with Bank ☾ Settlement to Merchant Account

8. Verify URL for Verifying the transaction through eazypay ID or PG Reference No

The Merchant can confirm the transaction status through online mode by passing following Parameters. The merchant can get the status using the combination of parameters mentioned below in the 3 options. In case the merchant does not receive the transaction details in the response due to network issues, the Verify URL can be used to check the status using only the Merchant ID and PG Reference No

For transactions where status is not received in real time, eazypay re-confirms the status up to 1 hour from the transaction time for the final confirmation.

Note:

Around 1-2% of transactions will become updated as success post 1 hr from the transaction initiated time. This can be up to a maximum of T+3 days from the transaction initiation time.

8.1.1 Option 1

Parameters: Eazypay Tran ID, Amount, Payment Mode, Merchant ID, Tran Date and Reference No

Request Packet

https://eazypay.icicibank.com/EazyPGVerify?ezpaytranid=1507171019414&amount=1&paymentmode=NET_BANKING_ICICI&merchantid=100001&trandate=20151106&pgreferenceno=123456

Response Packet

status=Challan Generated&ezpaytranid=1705191560702&amount=73&trandate=2017-05-19 17:51:51.0&pgreferenceno=4789&sdt=&BA=70&PF=15.00&TAX=18.00&PaymentMode=CASH

8.1.2 Option 2

Parameters: Amount, Payment Mode, Merchant ID, Tran Date and Reference No

Request Packet

https://eazypay.icicibank.com/EazyPGVerify?ezpaytranid=&amount=1&paymentmode=NET_BANKING_ICICI&merchantid=100001&trandate=20151106&pgreferenceno=123456

Response Packet

status=Challan Generated&ezpaytranid=1705191560702&amount=73&trandate=2017-05-19 17:51:51.0&pgreferenceno=4789&sdt=&BA=70&PF=15.00&TAX=18.00&PaymentMode=CASH

Note: In case of any error encountered while response from above options, only in this case the following URL should be used for transaction status

Request Packet

https://eazypay.icicibank.com/EazyPGVerify?ezpaytranid=&amount=&paymentmode=&merchantid=108714&trandate=&pgreferenceno=1605103046395

8.1.3 Option 3

Parameters: Merchant ID and Reference No or Merchant ID and Eazypay Transaction ID

Request Packet

https://eazypay.icicibank.com/EazyPGVerify?ezpaytranid=&amount=&paymentmode=&merchantid=100001&trandate=&pgreferenceno=123456

or

https://eazypay.icicibank.com/EazyPGVerify?ezpaytranid=1705191560702&amount=&paymentmode=&merchantid=100001&trandate=&pgreferenceno=

Response Packet

status=Challan Generated&ezpaytranid=1705191560702&amount=73&trandate=2017-05-19 17:51:51.0&pgreferenceno=4789&sdt=&BA=70&PF=15.00&TAX=18.00&PaymentMode=CASH

8.1.4 Verify URL Request Parameter Details

Ezpaytranid : eazypay Transaction ID for the transaction initiated in eazypay.

Amount : Transaction Total Amount

Paymentmode: CASH/CHEQUE/NET_BANKING/etc

Merchant ID : EazyPay Merchant ID allocated to the Merchant

Trandate : Transaction Date format in YYYYMMDD

Pgreferenceno: Reference no mapped to the eazypay Transaction ID

BA : Base Amount

PF : Processing Fee

TAX : Service Tax

Paymode : Payment Mode

8.1.5 Verify URL Response Parameter Details

Status=RIP

On Success confirmation from the transaction bank, the process of payment reconciliation between the respective bank and eazypay is initiated and the status will display as RIP (Reconciliation in Progress.)

Status=SIP

On successful reconciliation between the respective bank and eazypay, the status will change to SIP (Settlement in Progress)

Status=Success

On Successful settlement to the Merchant Account, the status will change to success.

Status=Challan Generated

Cash/Cheque/NEFTRTGS Challan Generated

Status=Transaction Initiated

If a payer has landed on the payment page but not initiated the transaction then the status will be transaction initiated.

Status=Cheque/DD In Clearance

When the branch has accepted the Non ICICI Cheque, but ICICI Bank has not received the confirmation from the respective banks, till the cheque is cleared and confirmed or payment is successful from any other payment mode, the status will be Cheque/DD In Under Clearance.

Status=Cheque/DD Returned

When the branch has accepted the Non ICICI Cheque and the cheque is not cleared and confirmed from respective banks, the status will be Cheque/DD Returned.

Status=FAILED

Once the payer has initiated the transaction and logged into respective payment modes on their bank site for Net-Banking or Debit Card/Credit Card and the transaction fails due to various reasons like, No Funds, Wrong Authentication, Session Expired, Canceled by User etc, for such transactions the status will be Failed.

Status=TIMEOUT

Once the Payer has initiated the transaction and logged into respective payment modes and the respective bank or Credit holder could not confirm the transaction in

a specific time for Net-Banking or Debit Card, Credit Card Aggregator site, such transactions will be marked as Transaction Timeout.

Status=Transaction Expired

Transaction Expired by the system.

Ezpaytranid : eazypay Transaction ID for the transaction initiated in eazypay.

Amount : Transaction Total Amount

Trandate : Transaction Date format in YYYYMMDD

Pgreferenceno: Reference no mapped to the eazypay Transaction ID

Sdt : Settlement Date

Optional Parameter in Verify URL

An optional parameter **(dstatus)** has been added to the Eazypay Verify URL. In case, the merchant does not want settlement update status (RIP and SIP) status to be shown and wants Success to be displayed instead for all such cases, the merchant can send "Y" in this parameter. Please note that the **Success response is subject to realization from the payer's bank account.**

Examples are mentioned below :

Request :

https://eazypay.icicibank.com/EazyPGVerify?ezpaytranid=18101115921584&amount=&paymentmode=&merchantid=113357&trandate=&pgreferenceno=&**dstatus=Y**

Response :

status=Success&ezpaytranid=18101115921584&amount=1.01&trandate=2018-10-11 10:25:44.0&pgreferenceno=&sdt=&BA=1&PF=0.01&TAX=0.0&PaymentMode=NET_BANKING_ICICI

Sending **Y** in this parameter will ensure that the merchant receives Success response instead of RIP and SIP which provide settlement status updates.