



INTEGRATION GUIDE FOR MERCHANTS

Version 4.2

09 May 2019

Copyright

This is unpublished, confidential document of TPS Pakistan Pvt Ltd.

No part of this document may be reproduced, stored in retrieval form, adopted or transmitted in any form or by any means, electronic, mechanical, photographic, graphic, optic or otherwise, translated in any language or computer language, without prior written permission from TPS Pakistan Pvt Ltd.

This document has been prepared with all due diligence, however, TPS, makes no representation or warranties with respect to the contents hereof and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this document and the accompanying information. Furthermore TPS, reserves the right to alter, modify or otherwise change in any manner the content hereof, without the obligation to notify any person of such revision or changes.

All registered and trademarked names referred to in this document are owned by their respective owners.

1. Document History

Date	Author	Status	Change Reference
15 th April 2014	Bina Khan and Faizan Ahmed	Added new sections for Confirmation/Reversal. Updated all sections for introducing Settlement Expiry and Confirmation flows.	Added: Section 9 and 7.3 Updated: Sections 6, 7 and Appendix 1.
22 nd April 2014	Usman Danish	Format, Appendix III fixed length	Updated section: 14
29 th April 2014	Mohammad Furqan Zakeria	Made Bank ID field as Mandatory in Payment Status Update	section 8.1
30 th April 2014	Bina Khan	Removed Customer IBAN fields and updated length of Bank ID field.	Sections 6.2 and 8.1.
7 th August 2014	Bina Khan	Removed Bill Reference parameter from Status Service. Removed other minor issues.	Sections 5.2, 6.1, 7.1, 7.2, 7.3, 8.1, 9, 9.1, 9.2
25 th December 2015	Adeel Siddiqui	Revision of document	Complete document
16 th June 2016	Adeel Siddiqui	Revision of Payment Status Update	Sections 8, 8.1, 8.2, 8.3
26 th July 2016	Iqbal Maskati	Addition of HMAC calculation	Sub section 11.2
16 th August, 2016	Muhammad Mujtaba	Set bank Id and product Id as optional in Payment inquiry and OTC update, added field CustomerCardNo And increase Auth code length to 12 in payment Status Inquiry Response.	Section 7.1 & 8.1, appendix 1
25 th August, 2016	Zia Ur Rehman	OTC Payment API Module	Section 11
09 th Sept, 2016	Iqbal Maskati	Status Update in All transaction types. Added response Codes	Section 8,14
6 th January, 2016	Muhammad Mujtaba	ASCII:32 will be used for white space in inquiry response	Section 7.2
24 th March, 2017	Muhammad Mujtaba	Added response code of 129. Modified transaction parameters with respect to discount module.	Section 6.1, 6.2, 11.1, 11.2 & 14
22 nd May, 2017	Muhammad Mujtaba	Added response code + Added documentation for Card API	Section 12, Section 15
31 July, 2017	Muhammad Mujtaba	Response code updated with respect to MPGS APIs	Section 15

	Muhammad Mujtaba	Setting txnexpiry in payment request as optional and update pp_description remarks	Section 6.1, Section 11.2
20 December,2018	Rabia Qaiser	<p>Added tokenization description for payment portal.</p> <p>Added pp_IsRegisteredCustomer, pp_TokenizedCardNumber in payment request.</p> <p>Added pp_IsRegisteredCustomer, pp_TokenizedCardNumber, pp_TokenizationResponseCode, pp_TokenizationResponseMsg, pp_CustomerCardNo, pp_CustomerCardExpiry in payment response.</p> <p>Rename response code field of existing table as Payment Response Code.</p> <p>Add new table for Tokenization Response Codes.</p>	<p>Section 5.2, Section 6.1,Section 6.2</p> <p>Section 15 Appendix I</p>
25 Feb 2019	Ali Abid Zaidi	Delete Token Api added	Section 13
27 Mar 2019	Ali Abid Zaidi	<p>Adding request fields pp_CustomerID, pp_CustomerEmail, pp_CustomerMobile</p> <p>Adding response fields pp_CustomerID, pp_CustomerEmail, pp_CustomerMobile</p> <p>Adding Instant Token Notification API.</p>	Section 6.1, Section 6.2, Section 13.2
04 April,2019	Idrees Shabbir	Retrieve Token Api added	Section 13.6
08 May,2019	Idrees Shabbir	<p>Following Apis are added</p> <ol style="list-style-type: none"> 1. Version2.0-PaymentAuthorize 2. Version2.0-PaymentAuthorize Token 3. Version2.0-Capture 	Section 12.1,12.2,12.3,12.4,12.5,12.6

Table of Contents

1. DOCUMENT HISTORY	3
TABLE OF CONTENTS	5
1. OVERVIEW	7
1.1 WHO SHOULD READ THIS GUIDE	8
1.2 RELATED DOCUMENTS	8
2. BUSINESS FLOW	9
2.1 PAYMENT METHODS FOR TRANSACTIONS:	9
2.2 DIRECT DEBIT TRANSACTION	11
3. MERCHANT SETUP PROCESS	12
4. PAYMENT GATEWAY TEST SYSTEM.....	13
5. ONLINE PAYMENTS OVER THE INTERNET	14
5.1 PAYMENT MODE SELECTION	15
5.2 PAYMENT PORTAL TRANSACTIONS	15
6. INTEGRATION WITH PG - PAYMENT PORTAL	17
6.1 PAYMENT PORTAL - INPUT PARAMETERS	17
6.1.1 Version 1.1	17
6.1.1 Version 1.2	20
6.1.2 Version 2.0	24
6.1.3 Optional Merchant Defined Fields	27
6.1.4 Optional Fields for Member Bank	27
6.2 PAYMENT PORTAL RESPONSE	28
6.2.1 Version 1.1	28
6.2.2 Version 1.2	31
6.2.3 Version 2.0	35
6.2.4 Optional fields	39
6.2.5 Optional Fields from Member Bank	39
6.3 RECEIVING THE TRANSACTION RESPONSE	39
7. PAYMENT STATUS INQUIRY	40
7.1 PAYMENT STATUS INQUIRY INPUT PARAMETERS	40
7.2 PAYMENT STATUS INQUIRY RESPONSE	41
7.3 PAYMENT STATUS INQUIRY PROCESSING	43
8. PAYMENT STATUS UPDATE	43
8.1 UPDATE PAYMENT STATUS INPUT PARAMETERS	44
8.2 UPDATE PAYMENT STATUS RESPONSE.....	46
8.3 UPDATE PAYMENT STATUS REITERATION.....	46
9. DELIVERY STATUS UPDATE	47
9.1 DELIVERY STATUS UPDATE INPUT PARAMETERS	47
9.2 DELIVERY STATUS UPDATE RESPONSE PARAMETERS	48
9.3 DELIVERY STATUS UPDATE PROCESSING	49

10. REFUND TRANSACTION	50
11. INTEGRATION WITH PG VIA PAYMENT API.....	50
11.1 PAYMENT API - INPUT PARAMETERS	50
11.2 PAYMENT API - REQUEST PARAMETERS	51
11.2.1 <i>Optional Merchant Defined Fields</i>	53
11.3 PAYMENT API RESPONSE.....	54
11.3.1 <i>Optional fields</i>	56
11.3.2 <i>Receiving Payment API Response</i>	56
11.4 SAMPLE API REQUESTS	57
11.4.1 <i>Sample Payment API Request from SOAP UI Tool</i>	57
11.4.2 <i>Sample Payment API Response</i>	57
12. INTEGRATION WITH CARD PAYMENT - API.....	58
12.1 PAYMENT AUTHORIZE -REQUEST JSON	58
Version 1.1	58
Version 2.0	59
12.2 PAYMENT AUTHORIZE -RESPONSE JSON	60
Version 1.1	60
Version 2.0	60
12.3 PAYMENT AUTHORIZE VIA TOKEN -REQUEST JSON	61
Version 2.0	61
12.4 PAYMENT AUTHORIZE VIA TOKEN-RESPONSE JSON	62
Version 2.0	62
12.5 PAYMENT CAPTURE -REQUEST JSON	63
Version 1.1	63
Version 2.0	63
12.6 PAYMENT CAPTURE -RESPONSE JSON	64
Version 1.1	64
Version 2.0	64
12.7 PAYMENT VOID -REQUEST JSON.....	65
12.8 PAYMENT VOID -RESPONSE JSON.....	65
12.9 PAYMENT REFUND -REQUEST JSON.....	65
12.10 PAYMENT REFUND -RESPONSE JSON.....	66
12.11 PAYMENT RETRIEVE - REQUEST JSON	66
12.12 PAYMENT RETRIEVE -RESPONSE JSON	67
12.13 CHECK 3DS ENROLLEMENT -REQUEST JSON	67
Version 1.1	67
Version 2.0	68
12.14 CHECK 3DS ENROLLEMENT -RESPONSE JSON	68
Version 1.1	68
Version 2.0	69
12.15 PROCESS ACS-REQUEST JSON	70
Version 1.1	70
Version 2.0	70
12.16 PROCESS ACS -RESPONSE JSON	72
Version 1.1	72
Version 2.0	73
12.17 PAYMENT DIRECT PAY -REQUEST JSON.....	73
Version 1.1	73
Version 2.0	74

12.18 PAYMENT DIRECT PAY -RESPONSE JSON.....	75
Version 1.1	75
Version 2.0.....	75
13. TOKENIZATION API	76
13.1 DELETE TOKEN API.....	76
13.2 INSTANT TOKEN NOTIFICATION (ITN).....	77
Version 1.0	77
13.3 CHECK3DSENVIRONMENTVIA TOKEN	78
Version 2.0	78
13.4 PROCESSACSVIA TOKEN.....	81
Version 2.0	81
13.5 PAYVIA TOKEN	83
Version 2.0	83
13.6 RETRIEVE TOKEN	86
14. CALCULATING AND VALIDATING THE SECURE HASH	87
14.1 HOW THE SECURE HASH IS CREATED AND VERIFIED.....	87
14.2 HOW IS SHA256- HMAC CALCULATED	88
15. PADDING RULES	90
16. APPENDIX I - RESPONSE CODE.....	90
17. APPENDIX II- AMOUNT VALUES FOR GENERATING DIFFERENT RESPONSE IN TEST ENVIRONMENT.....	93
18. APPENDIX III - FIXED LENGTH	94

1. Overview

This *Payment Gateway Integration Guide for Merchants* is a technical integration document for Merchants to interface with PMCL Payment Gateway (PG) allowing their customers to perform e-commerce transactions over the internet.

It guides merchant on how to use various functionality of the Payment Portal Integration and describes the interfacing specification of Version 1.1 of Payment Gateway Portal.

The Merchant can enable multiple modes of payment over their e-commerce website with this integration:

- Debit Card
- Over the counter
- Mobile Wallet
- Direct Debit (Internet Call to customer's Banking portal)
- Account

Furthermore, the guide also elaborates on the business logic and transaction flow of payment processing done through the Payment Gateway with respect to the new interface for payment processing.

1.1 Who Should Read This Guide

The Payment Gateway's Payment Portal provides the online merchants an easy to use interface enabling them to process transactions over their e-commerce websites. The interfacing is done through standard web technologies and requires minimal development at the merchant end. Moreover, Payment Portal does not require any software to be installed at the merchant end and allows the merchants to leverage their existing infrastructure and applications to enable transaction processing through Payment Gateway.

The document is intended for application developers and business analysts at merchant to allow them to integrate effectively with the Payment Gateway Portal Interface.

1.2 Related Documents

A Merchant Portal by Payment gateway is also available to all merchants in addition to Payment Portal Interface. The Merchant Portal offers a variety of back-office features related to merchant administration of Payment Gateway. For complete details *Payment Gateway Merchant Portal Guide* may be referenced.

2. Business Flow

This section describes the business transaction flow or the customer experience during payment cycle using Debit Card and Direct Debit option. It is designed to highlight the transaction handling at Merchant portal and responsibilities shared between Merchant and Payment Gateway during the online end-to-end cycle:

2.1 Payment Methods for Transactions:

The online user experience will be divided between two portals:

1. Merchant's Web site
2. Payment Gateway

Merchant's Web Site:

The merchant's portal will prepare the item cart and offer the check-out option to the customer. The transaction flow and information captured are as follows:

1. **Product Selection:** The customer selects one or more products to be bought from the merchant
2. **Product Details:** Upon check-out the merchant confirms the items to be purchased
3. **Product Payment Details:** An invoice will be presented to the customer that includes the price of each product and the total amount payable

***Note:** If the merchant is integrated with multiple payment gateways then the following step (4) will be presented otherwise the customer will be redirected to the Payment Gateway*

4. **Payment Method:** If the merchant is integrated with multiple payment gateways the customer will be prompted to select a payment method. If the customer chooses to pay by debit card, direct debit, mobile wallet or over the counter then he will be redirected to the Payment Gateway.

Payment Gateway:

The Payment Gateway will receive control from the merchant portal, based on the transaction options selected at merchant end. Following will be the customer experience:

Payment Method Selection: This screen will be shown to customer if Merchant did offer Payment Method Selection (4) at its end.

Customer will be presented with Payment Method Selection covering debit card, direct debit, mobile wallet, account or over the counter.

1. Debit Card:

Card Number: Customer will enter his/her card number on Payment Gateway

Expiry & CVV2: Next screen will ask user to enter his Expiry & CVV2, once confirm is clicked the transaction will be posted to relevant system for authorization

Note: In case of link cards only CVV2 will asked from customer at the time of transactions for registered customer.

Payment Gateway - Transaction Completion: Upon successful authorization, payment gateway will prompt of success status and offer customer the option to register for future transactions

Merchant Confirmation Page: Customer will be taken back to return URL of the merchant

2. Mobile Wallet:

Mobile Number (MSISDN): Customer will enter his mobile number, once confirm is clicked the transaction will be posted to relevant system for authorization.

Note: In case of linked mobile wallets confirmation will be sent by CPS for registered customer.

3. Over the Counter:

Customer will be shown with a 12 digit voucher number for payment at any outlet.

4. Account:

Customer will be asked to select bank, enter his/her account number with CNIC. An OTP will be generated by issuer bank on customer's registered mobile number and he/she will be asked to enter the same on screen. PGW will capture the OTP and send the request for authorization.

2.2 Direct Debit Transaction

The online user experience will be divided between three portals:

1. Merchant's Web site
2. Payment Gateway
3. Bank's Internet Banking

Merchant's Web Site:

The merchant's portal will prepare the item cart and offer the check-out option to the customer. The transaction flow and information captured are as follows:

1. **Product Selection:** The customer selects one or more products to be bought from the merchant
2. **Product Details:** Upon check-out the merchant confirms the items to be purchased
3. **Product Payment Details:** An invoice will be presented to the customer that includes the price of each product and the total amount payable

Note: If the merchant is integrated with multiple payment gateways then the following step (4) will be presented otherwise the customer will be redirected to the Payment Gateway

5. **Payment Method:** If the merchant is integrated with multiple payment gateways the customer will be prompted to select a payment method. If the customer chooses to pay by debit card, direct debit, mobile wallet or over the counter then he will be redirected to the PMCL Payment Gateway.

Payment Gateway:

The Payment Gateway will receive control from the merchant portal, based on the transaction options selected at merchant end; there are two landing pages of Payment Gateway. Following will be the customer experience:

Payment Method Selection: This screen will be shown to customer if Merchant did offer Payment Method Selection (4) at its end.

Customer will be presented with Payment Method Selection covering debit card, direct debit, mobile wallet or over the counter.

OR

Page Redirect Prompt Page: Customer will be prompted with the message of being redirected to its bank portal for transaction

completion. This can be a silent page and may be skipped, while customer is transferred to banking portal.

Bank's Internet banking:

1. **Bank's Direct Debit Portal:** The Payment Gateway will transfer control of the customer to the selected bank's Web
2. **Enter Credentials:** To log in the customer must enter his/her internet banking user name and password
3. **Confirmation:** Once authenticated, bank will display the details of the current transaction and the customer asked to confirm the details or authorize payment
4. **Payment Information:** Payment related details will be shown to customer
5. **Page Redirect PG:** bank redirects the customer back to the Payment Gateway (this page may be 'silent')
6. **Merchant Confirmation Page:** The Payment Gateway returns the Customer to the URL specified by the merchant

3. Merchant Setup Process

In order to process online payments using the Payment Gateway, the merchant needs to be registered with the Payment Gateway as member merchant.

The below process assumes that the merchant has been registered and all the parameters related to merchant have been configured in the Payment Gateway system.

1. Once merchant has registered for Payment Gateway services, the merchant will be provided with *Payment Gateway Integration Guide for Merchants* and *Merchant Portal User Guide* documents. These documents will assist in integrating with the Payment Gateway Payment Portal and elaborate the administration support processes. The integration documents contain the following:
 - a. Payment Gateway Payment Portal Integration Guide
 - b. Sample code for integration
2. At the time of merchant registration with the Payment Gateway, an ID will be assigned to each merchant. In addition Payment Gateway will generate two codes:
 - a. **Access Code**
Along with the Merchant ID, the Access Code is used to identify the merchant

This value is emailed to the registered email address of the Merchant at the time of merchant registration. The merchant may request to re-generate the codes by communicating with the Payment Gateway service provider.

3. After getting the basic information, the merchant will be in a position to perform test transaction using the sample code provided. Once the sample transaction has been successfully processed it indicates that all the required systems have been configured correctly and the merchant is ready to go.
4. Now that the merchant creation and configuration has been validated, merchant can now start with its integration development. Merchant should follow the rules described later in the document to integrate and payment-enable its e-commerce website.
5. After developing required capability in its e-commerce website for integrating with Payment Portal, merchant will be ready to perform testing the payment processing through the Payment Portal. Merchant should coordinate with its Payment Gateway service provider to validate that testing has been successful.
6. To test integration of merchant's e-commerce portal with the Payment Gateway, merchant will be required to connect with PG test system IP address provided by its service provider. The details of how to connect and perform different test cases is described later in the document.

Below mentioned URL will be utilized

["http://localhost/MerchantPortal/transactionmanagement/merchantform"](http://localhost/MerchantPortal/transactionmanagement/merchantform)

* In place of localhost test environment IP should be placed

7. Finally after the transaction testing has been successfully done, merchant can move its system into production. It is to be noted that merchant will need to inform the service provider before merchant will be able to accept transaction in the production environment.

4. Payment Gateway Test System

Payment Gateway provides an independent testing system but has the same infrastructure as production. This testing facility caters for all the merchant integration features.

The merchant is provided with IP addresses to connect with the test and production systems as required. In order for a merchant to use the testing environment, the merchant connects with the Payment Gateway Test System IP address. Moreover, when connecting with the test system the merchant is required to prefix the provided Merchant ID with the word 'Test'. This is to ensure that merchant does not accidentally connect the test system with production or vice versa. Please note that in case the merchant provides

Merchant ID without prefix 'Test' to the test system, the transaction will be rejected and will not be processed.

As mentioned earlier the test environment is a complete system and provides all the options. The transactions are recorded in the system and the merchant can access the reports and other administration options via the Test Merchant Portal.

In case of testing, the transactions are being authorized by a simulator, therefore in order to generate different responses from the Payment Gateway the merchant can send different transaction amounts. For example, an amount of PKR 100.00 sent to the payment gateway will generate transaction successfully processed response, whereas amount of PKR 101.00 will generate invalid card number response. This will allow the merchant to verify proper exception handling at its end. The complete list of response codes can be found in Appendix I and list of amounts corresponding to response codes for testing are available in Appendix II.

As test transactions are fully recorded, Merchants can test PG's Payment Status Inquiry service. In case of Direct Debit, PG hits Bank's service for inquiry. If bank is not available for testing, PG will respond with response message corresponding to the original amount of the transaction in question. The list of amounts corresponding to response codes for testing is available in Appendix II.

PG test system will also provide Update Payment Status service for testing. For this purpose a web page will be made accessible to Merchants through which they can invoke PG's Update Payment Status service.

Once the testing has been completed, the merchant can move the testing application into production. Please note that the merchant will be required to configure the integration options with Payment Gateway so that the merchant portal now connects with the Payment Gateway Production system. Moreover, the prefix of 'Test' should be removed when posting transactions in the production environment.

Further, the merchant cannot perform live transactions unless configured in Payment Gateway production system to do so.

5. Online Payments over the Internet

Payment Gateway allow merchants to enable online payment processing over their e-commerce portals in a secure and easy to use manner. This guide focuses on integration details for merchant to integrate with Payment Gateway in order to allow transaction processing via the Payment Gateway Payment Portal for

- Debit Card
- Mobile Wallets
- Over the counter - OTC
- Direct Debit (Internet Call to customer's Banking portal)

The Payment Gateway Payment Portal provides payment processing and transaction status inquiry facilities. In addition to the Payment Gateway Payment Portal, a merchant

administration portal is also made available to the merchants, the details of which can be found in the Merchant Portal Guide.

5.1 Payment Mode Selection

Payment Gateway Payment Portal provides flexibility to the merchants by providing the option of allowing Payment Mode Selection on Payment Gateway.

Payment mode selection can be handled at Payment Gateway landing page.

Please note that PMCL will enable the Payment Gateway services for all banks.

Steps for handling selection at merchant site:

1. Once customer is redirected from merchant portal, customer will be on landing page where customer can login as registered or make the payment as unregistered. Redirection of customer will be made using HTTPs protocol.
2. Customer will select the payment options provided after login of customer. Following are the payment options available for transaction processing.
 - a. Debit Card
 - b. Over the counter
 - c. Mobile Wallet
 - d. Direct Debit

5.2 Payment Portal Transactions

The Payment Gateway Payment Portal provides online transaction processing and authorization facility. The Payment Portal provides the following four types of transactions:

1. Debit Card Purchase Transaction - Payment Portal

This is provided via the online web page hosted by the Payment Gateway. The merchant provides the transaction details (transaction amount, order number, etc.) to the Payment Page, the Payment Page in turn takes the user's card details and then performs online transaction authorization and returns the response to the merchant portal. The details of the function are described in later sections.

Tokenization:

Tokenization allows you to store card payment details in exchange for a token. The token replaces the card details in the transaction request sent to the gateway. This is useful as the gateway handles the payment details collected from the payer thereby reducing your PCI compliance obligations. Further, if the token is stored with the payer data, it may be used when the

payer returns to make another purchase. Additional parameters can be accessible for tokenization from version 1.2 and onwards.

2. Direct Debit

This transaction enables a customer to make a transaction using an internet banking account of member bank. A merchant provides transaction details (transaction amount, order number, etc.) to the Payment Gateway, the Payment Page redirects the customer to the respective member bank's designated internet banking page. The customer will login to the internet banking portal using his credentials and complete the transaction. The member bank will then return the response to the payment gateway which in turn will forward it to the merchant portal. The details of the function are described in later sections.

3. Over the Counter

This transaction enables a customer to make a transaction by providing the cash to any mobicash outlet. Customer will have a voucher number of 12 digits. Customer will visit mobicash outlet and will pay the desired amount.

4. Mobile Wallet

This is provided via the online web page hosted by the Payment Gateway. The merchant provides the transaction details (transaction amount, order number, etc.) to the Payment Page, the Payment Page in turn takes the mobile wallet of customer.

5. Payment Status Inquiry

Payment Status Inquiry is a web service interface exposed by the Payment Gateway which allows merchant to query the status of any transaction that has been performed through the merchant website using the Payment Gateway. The merchant can query against the transaction reference id. This function will be used by merchant to query status of any transaction type. The details of the function are described in later sections.

6. Payment Status Update

Payment Status Update web service is to be exposed by Merchants so that Payment Gateway can update the status of a pending transaction. Parameter details and signature of the function are described in later sections.

7. Delivery Status Service

Delivery Status Service is a web service interface exposed by the Payment Gateway which is to be invoked by the merchant to confirm

the delivery of services or goods. The details of the function are described in later sections.

6. Integration with PG - Payment Portal

For merchants to enable payment processing through Payment Gateway, they are required to integrate with the Payment Gateway Payment Portal. This section describes in detail how to integrate the merchant e-commerce website with the PG Payment Portal.

Merchant will provide the input parameters using an HTTP POST request to the PG Payment Portal. The PG Payment Portal will process transaction and return the response via an HTTP POST request to the URL provided by the merchant. The merchant may use the response to show the transaction results (success or failure) of the transaction to the customer.

6.1 Payment Portal - Input Parameters

The PG Payment Portal will receive an HTTP POST request from the merchant website which will contain the merchant authentication details along with the transaction details. The Payment Gateway will inquire the required details from the customer and process transaction. The form will be containing the input parameters as hidden fields such as:

```
<input type="hidden" id="pp_Version" value="1.0">
<input type="hidden" id="pp_TxnType" value="PAY">
<input type="hidden" id="pp_MerchantID" value=" MERC001">
<input type="hidden" id="pp_TxnRefNo" value="TXN1234">
<input type="hidden" id="pp_Amount" value="10000">
<input type="hidden" id="pp_TxnDateTime" value="20110909124545">
....
```

The parameter names and details of each parameter are described below:

6.1.1 Version 1.1

This version is used to perform basic payments. Card tokenization functionality is not present in this version

Parameter	Max. Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.1	Payment Portal Version. Fixed value '1.1', '1.2' or '2.0' should be used
pp_TxnType	10 AN	No	PAY	Presents the transaction type: <ul style="list-style-type: none"> Transactions via Internet Banking = DD Mobile Wallet = MWALLET

				Master Card = MIGS Over The Counter = OTC Debit Card = PAY
pp_Language	3 A	Yes	EN	Specifies the language in which to display the page. Fixed value 'EN'.
pp_MerchantID	10 AN	Yes	MERC001	Unique Id assigned to each Merchant by PG.
pp_SubMerchantID	10 AN	No	SUBMER001	If the merchant is handling any child merchants at its end, then the child merchant Id will be provided. The Transaction reports will be grouped on the basis of Sub Merchant Id, if available.
pp_Password	10 AN	Yes	75019F19EA	Password is assigned to each merchant and is used to authenticate merchant at the time of payment. Password is a system generated value.
pp_BankID	4AN	No	BNK01	This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field. Bank Id of the customer's banks if available.
pp_ProductID	4 A	No	RETL	This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field. Product of Bank through which payment will be done. For e.g. Retail, Corporate. Fixed values: 'RETL', 'CORP'
pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx2011090901	A unique value created by the merchant to identify the transaction.
pp_Amount	13 N	Yes	100.00 will be passed as 10000	The transaction amount. Please note that no decimal places are included. Decimal place will be assumed at the default position of the currency provided.
pp_DiscountedAmount	13 N	No	100.00 will be passed as 10000	The discounted amount merchant wants to send. Please note that no decimal places are included. Decimal place will be assumed at the

				default position of the currency provided.
pp_DiscountBank	4AN	No	SCB	BankID of the bank for which merchant wish to send discount.
pp_TxnCurrency	3 A	Yes	PKR	Currency of Transaction amount. It has a fixed value 'PKR'.
pp_TxnDateTime	14 N	Yes	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	Merchant provided date and time of transaction. The format of date time should be yyyyMMddHHmmss.
pp_BillReference	20 AN & '.'	Yes	Cart001	Bill/invoice Number being settled.
pp_Description	200 Free Text Field	Yes	Payment for 3 Item(s) bought	Transaction details to be shown on screen as desired by the merchant. This field will be parsed to identify any malicious data entered by the end user. In cases when any of these characters <>*=%/:"{} are inserted, they will be replaced with a space. Pipe ' ' is not allowed
pp_TxnExpiryDateTi me	14 N	No	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	Transaction Expiry can be specified by merchant to indicate to the issuing bank that the transaction must be approved within this period. Please note that the default and maximum value of this expiry is 3 months.
pp_ReturnURL	200 AN	Yes	Merchant site/payme nt/Results. aspx	The URL where merchant wants the transaction results to be shown. Once the transaction has been processed, response details will be sent over to the merchant on this URL using an HTTP POST Request. Part of this URL is to be provided to PMCL before transaction processing starts. This part URL will be used by the PG to ensure that all responses are sent to an authentic URL.
pp_SecureHash	64 AN	No	9e107d9d372bb6826bd81d3542a419d69e107d9d372bb682	Used to allow the Payment Gateway to check the integrity of the transaction request.

			6bd81d354 2a419d6	
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+{}“:’?><	No		Optional Fields Merchant can send additional information to PG in this field. These will be returned to Merchant in transaction response. xxxx in the name for Optional fields can be replaced by any set of characters.
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+{}“:’?><	No		
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+{}“:’?><	No		
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+{}“:’?><	No		
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+{}“:’?><	No		
ppmbf_xxxx	255 AN	No		Optional Fields Merchant may send some additional information to Member Bank. If received, PG will forward the information contained in this field to bank. xxxx in the name for Optional fields can be replaced by any set of characters.
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		

6.1.1 Version 1.2

This version was introduced to support tokenization. It is deprecated and not in use further.

Parameter	Max. Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.2	Payment Portal Version. Fixed value ‘1.1’, ‘1.2’ or ‘2.0’ should be used

pp_TxnType	10 AN	No	PAY	<p>Presents the transaction type:</p> <ul style="list-style-type: none"> Transactions via Internet Banking = DD Mobile Wallet = MWALLET Master Card = MIGS Over The Counter = OTC Debit Card = PAY
pp_Language	3 A	Yes	EN	<p>Specifies the language in which to display the page.</p> <p>Fixed value 'EN'.</p>
pp_IsRegisteredCustomer	3 A	Yes	Yes	<p>This parameter can be accessible from 1.2 version. It represents that the request has been made by the registered or a guest customer of a merchant.</p>
pp_TokenizedCardNumber	16 N	No	9113633378227378	<p>This parameter can be accessible from 1.2 version. It represents the tokenized card number of returning customer.</p> <p>This token will be received to the merchant in response of save card details when selected by the customer on Payment portal.</p>
pp_MerchantID	10 AN	Yes	MERC001	<p>Unique Id assigned to each Merchant by PG.</p>
pp_SubMerchantID	10 AN	No	SUBMER001	<p>If the merchant is handling any child merchants at its end, then the child merchant Id will be provided. The Transaction reports will be grouped on the basis of Sub Merchant Id, if available.</p>
pp_Password	10 AN	Yes	75019F19EA	<p>Password is assigned to each merchant and is used to authenticate merchant at the time of payment. Password is a system generated value.</p>
pp_BankID	4AN	No	BNK01	<p>This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field.</p> <p>Bank Id of the customer's banks if available.</p>
pp_ProductID	4 A	No	RETL	<p>This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field.</p> <p>Product of Bank through which payment will be done. For e.g. Retail, Corporate.</p>

				Fixed values: 'RETL', 'CORP'
pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx20110909 01	A unique value created by the merchant to identify the transaction.
pp_Amount	13 N	Yes	100.00 will be passed as 10000	The transaction amount. Please note that no decimal places are included. Decimal place will be assumed at the default position of the currency provided.
pp_DiscountedAmount	13 N	No	100.00 will be passed as 10000	The discounted amount merchant wants to send. Please note that no decimal places are included. Decimal place will be assumed at the default position of the currency provided.
pp_DiscountBank	4AN	No	SCB	BankID of the bank for which merchant wish to send discount.
pp_TxnCurrency	3 A	Yes	PKR	Currency of Transaction amount. It has a fixed value 'PKR'.
pp_TxnDateTime	14 N	Yes	9 th Oct, 2011 10:35:47 PM will be sent as '201110092 23547'	Merchant provided date and time of transaction. The format of date time should be yyyyMMddHHmmss.
pp_BillReference	20 AN & '.'	Yes	Cart001	Bill/invoice Number being settled.
pp_Description	200 Free Text Field	Yes	Payment for 3 Item(s) bought	Transaction details to be shown on screen as desired by the merchant. This field will be parsed to identify any malicious data entered by the end user. In cases when any of these characters <>*=%/:"{} are inserted, they will be replaced with a space. Pipe ' ' is not allowed
pp_TxnExpiryDateTi me	14 N	No	9 th Oct, 2011 10:35:47 PM will be sent as '201110092 23547'	Transaction Expiry can be specified by merchant to indicate to the issuing bank that the transaction must be approved within this period. Please note that the default and maximum value of this expiry is 3 months.

pp_ReturnURL	200 AN	Yes	Merchant site/payment/Results.aspx	<p>The URL where merchant wants the transaction results to be shown. Once the transaction has been processed, response details will be sent over to the merchant on this URL using an HTTP POST Request.</p> <p>Part of this URL is to be provided to PMCL before transaction processing starts. This part URL will be used by the PG to ensure that all responses are sent to an authentic URL.</p>
pp_SecureHash	64 AN	No	9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6	Used to allow the Payment Gateway to check the integrity of the transaction request.
ppmpf_xxxx	255 AN and ~!@#\$%^&*() _+{}“:’?><	No		<p>Optional Fields</p> <p>Merchant can send additional information to PG in this field. These will be returned to Merchant in transaction response.</p> <p>xxxx in the name for Optional fields can be replaced by any set of characters.</p>
ppmpf_xxxx	255 AN and ~!@#\$%^&*() _+{}“:’?><	No		
ppmpf_xxxx	255 AN and ~!@#\$%^&*() _+{}“:’?><	No		
ppmpf_xxxx	255 AN and ~!@#\$%^&*() _+{}“:’?><	No		
ppmpf_xxxx	255 AN and ~!@#\$%^&*() _+{}“:’?><	No		
ppmbf_xxxx	255 AN	No		<p>Optional Fields</p> <p>Merchant may send some additional information to Member Bank.</p> <p>If received, PG will forward the information contained in this field to bank.</p> <p>xxxx in the name for Optional fields can be replaced by any set of characters.</p>
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		

ppmbf_xxxx	255 AN	No		
------------	--------	----	--	--

6.1.2 Version 2.0

This version is used to support payment with tokenized approach. In this approach, token will be shared with merchant through token generation notification.

Parameter	Max. Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	2.0	Payment Portal Version. Fixed value '1.1', '1.2' or '2.0' should be used
pp_TxnType	10 AN	No	PAY	Presents the transaction type: <ul style="list-style-type: none"> Transactions via Internet Banking = DD Mobile Wallet = MWALLET Master Card = MIGS Over The Counter = OTC Debit Card = PAY
pp_Language	3 A	Yes	EN	Specifies the language in which to display the page. Fixed value 'EN'.
pp_IsRegisteredCustomer	3 A	Yes	Yes	This parameter can be accessible from 1.2 version. It represents that the request has been made by the registered or a guest customer of a merchant.
pp_TokenizedCardNumber	16 N	No	9113633378227378	This parameter can be accessible from 1.2 version. It represents the tokenized card number of returning customer. This token will be received to the merchant in response of save card details when selected by the customer on Payment portal.
pp_MerchantID	10 AN	Yes	MERC001	Unique Id assigned to each Merchant by PG.
pp_SubMerchantID	10 AN	No	SUBMER001	If the merchant is handling any child merchants at its end, then the child merchant Id will be provided. The Transaction reports will be grouped on the basis of Sub Merchant Id, if available.

pp_Password	10 AN	Yes	75019F19EA	Password is assigned to each merchant and is used to authenticate merchant at the time of payment. Password is a system generated value.
pp_BankID	4AN	No	BNK01	This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field. Bank Id of the customer's banks if available.
pp_ProductID	4 A	No	RETL	This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field. Product of Bank through which payment will be done. For e.g. Retail, Corporate. Fixed values: 'RETL', 'CORP'
pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx2011090901	A unique value created by the merchant to identify the transaction.
pp_Amount	13 N	Yes	100.00 will be passed as 10000	The transaction amount. Please note that no decimal places are included. Decimal place will be assumed at the default position of the currency provided.
pp_DiscountedAmount	13 N	No	100.00 will be passed as 10000	The discounted amount merchant wants to send. Please note that no decimal places are included. Decimal place will be assumed at the default position of the currency provided.
pp_DiscountBank	4AN	No	SCB	BankID of the bank for which merchant wish to send discount.
pp_TxnCurrency	3 A	Yes	PKR	Currency of Transaction amount. It has a fixed value 'PKR'.
pp_TxnDateTime	14 N	Yes	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	Merchant provided date and time of transaction. The format of date time should be yyyyMMddHHmmss.
pp_BillReference	20 AN & '.'	Yes	Cart001	Bill/invoice Number being settled.

pp_Description	200 Free Text Field	Yes	Payment for 3 Item(s) bought	Transaction details to be shown on screen as desired by the merchant. This field will be parsed to identify any malicious data entered by the end user. In cases when any of these characters <>*=%/:"{} are inserted, they will be replaced with a space. Pipe ' ' is not allowed
pp_TxnExpiryDateTIme	14 N	No	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	Transaction Expiry can be specified by merchant to indicate to the issuing bank that the transaction must be approved within this period. Please note that the default and maximum value of this expiry is 3 months.
pp_ReturnURL	200 AN	Yes	Merchant site/payment/Results.aspx	The URL where merchant wants the transaction results to be shown. Once the transaction has been processed, response details will be sent over to the merchant on this URL using an HTTP POST Request. Part of this URL is to be provided to PMCL before transaction processing starts. This part URL will be used by the PG to ensure that all responses are sent to an authentic URL.
pp_SecureHash	64 AN	No	9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6	Used to allow the Payment Gateway to check the integrity of the transaction request.
pp_CustomerID	255 AN	No	(Provided by Merchant)	Registered Customer's LoginID or Identifier address provided by Merchant. This field can be accessible in payment version 2.0
pp_CustomerEmail	255 AN and !#\$%&'*+,-/=^_`{ }~	No	sample@gmail.com	Registered Customer's Email address provided by Merchant. This field can be accessible in payment version 2.0.
pp_CustomerMobile	11 N	No	03001237896	Registered Customer's Mobile Number provided by Merchant. This field can be accessible in payment version 2.0.

ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+}{"':?><	No		Optional Fields Merchant can send additional information to PG in this field. These will be returned to Merchant in transaction response. xxxx in the name for Optional fields can be replaced by any set of characters.
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+}{"':?><	No		
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+}{"':?><	No		
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+}{"':?><	No		
ppmpf_xxxx	255 AN and ~!@#\$\$%^&*() _+}{"':?><	No		
ppmbf_xxxx	255 AN	No		Optional Fields Merchant may send some additional information to Member Bank. If received, PG will forward the information contained in this field to bank. xxxx in the name for Optional fields can be replaced by any set of characters.
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		

6.1.3 Optional Merchant Defined Fields

PG Payment Portal also supports up to 5 merchant defined fields that will be returned to the merchant in transaction response.

These fields must be less than or equal to 255 bytes and must start with ppmpf_. These fields will only be exchanged during HTTP POST request/response and will not be available in any of the web services, Merchant Back Office portal or reports etc.

6.1.4 Optional Fields for Member Bank

Merchant may be required to forward some specific information to Member Bank. To facilitate this operation PG Payment Portal also supports up to 5 merchant defined fields that will be forwarded to the member bank as part of the direct debit request.

These fields must be less than 255 bytes and must start with ppmbf_. These optional fields, if sent, will be part of the secure hash.

These fields are only forwarded to the Member Bank in case of Direct Debit transactions. In case of other transaction type, these fields will be ignored.

6.2 Payment Portal Response

The response by Payment Gateway Payment Portal will send the transaction results to the merchant portal so that the merchant can perform the required operations accordingly.

The details will be forwarded to the URL provided in the pp_ReturnURL using an HTTP POST Request. The response parameters returned by the Payment Portal are described below.

6.2.1 Version 1.1

This version is deprecated and shall not be used by new merchants that are onboarding.

Parameter	Max. Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.1	As provided in the request.
pp_TxnType	10 AN	No	PAY	As provided in the request.
pp_IsregisteredCustomer	3 A	Yes	Yes/No	As provided in the request.
pp_Language	3 A	Yes	EN	As provided in the request.
pp_MerchantID	10 AN	Yes	MERC001	Unique Id assigned to each Merchant by PG.
pp_SubMerchantId	10 AN	No	SUBMERO01	As provided in the request.
pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx2011090901	As provided in the request.
pp_Amount	13 N	Yes	100.00 will be passed as 10000	If merchant wish to use discount module than final amount will be respond back which payaxis considers, else same amount will be responded as in the request.
pp_TxnCurrency	3 A	Yes	PKR	As provided in the request.
pp_TxnDateTime	14 N	Yes	9 th Sept, 2011 10:35:47 PM will	As provided in the request.

			be sent as '20110909203547'	
pp_BillReference	20 AN & '.'	Yes	Cart001	As provided in the request.
pp_ResponseCode	3 AN	Yes	000	Response code representing the transaction success or failure. A response code of 000 represents success. For a complete list of response codes refer to Appendix I.
pp_CustomerCardExpiry	4 N	Yes	0220	This parameter can be accessible from 1.2 version. This field represents the customer card expiry against tokenized card. Example : 0220 = Feburay 2020
pp_ResponseMessage	200 AN	No	Not enough balance to perform transaction	Error details in case the transaction failed to be processed. This field will be mandatory for all cases where response code is not equal to 000.
pp_RetreivalReferenceNo	12 N	No	000112233445	A unique number generated by the Payment Gateway when the transaction got processed. The number should be stored and used for future reference. The number is unique for any given date.
pp_AuthCode	12 N	No	123456	An identifying code issued by the issuing bank to approve or deny the transaction. The field is mandatory in case of successful response code. Refer to Appendix I for a list of response codes and the codes which when sent will require Auth Code.
pp_SettlementExpiry	14N	No	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	A date supplied by the Payment Gateway indicating that if the merchant does not send a Confirmation of the transaction by this time, the PG will mark the transaction as expired and the Merchant will not be able to resume it.

				The field is mandatory in case of successful response code and when the AuthCode is not blank.
pp_BankID	4 AN	Yes	BNK1	Customer's bank that authorized the transaction.
pp_ProductID	4 A	No	RETL	<p>This field will only be used in case of DD transaction type. Product of Bank through which payment has been performed. For e.g. Retail, Corporate.</p> <p>Fixed values: 'RETL', 'CORP'</p> <p>In case value was provided at the time of request, this field will contain the same value. Otherwise, ID of the product chosen by customer at PG will be filled.</p>
pp_SecureHash	64 AN	No	9e107d9d 372bb682 6bd81d35 42a419d6 9e107d9d 372bb682 6bd81d35 42a419d6	Used to allow the Merchant to check the integrity of the transaction response.
ppmpf_xxxx	255 AN	No		<p>Optional Fields</p> <p>Merchant can send additional information to PG in these fields while making the payment request. If received, the fields will be echoed back at the time of response.</p>
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		

ppmbf_xxxx	255 AN	No		Optional Fields Member Bank may send some additional information to Merchant. If received from Member Bank, PG will forward the information contained in this field to Merchant.
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		

Note: xxxx in the name for Optional fields can be replaced by any set of characters.

6.2.2 Version 1.2

This version is deprecated and shall not be used for new merchant's onboarding

Parameter	Max. Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.1	As provided in the request.
pp_TxnType	10 AN	No	PAY	As provided in the request.
pp_IsregisteredCustomer	3 A	Yes	Yes/No	As provided in the request.
pp_Language	3 A	Yes	EN	As provided in the request.
pp_MerchantID	10 AN	Yes	MERC001	Unique Id assigned to each Merchant by PG.
pp_SubMerchantId	10 AN	No	SUBMERO01	As provided in the request.
pp_TxnRefNo	20 AN & '/' & ','	Yes	Tx2011090901	As provided in the request.
pp_Amount	13 N	Yes	100.00 will be passed as 10000	If merchant wish to use discount module than final amount will be respond back which payaxis considers, else same amount will be responded as in the request.
pp_TxnCurrency	3 A	Yes	PKR	As provided in the request.
pp_TxnDateTime	14 N	Yes	9 th Sept, 2011 10:35:47 PM will be sent	As provided in the request.

			as '2011090 9203547'	
pp_BillReference	20 AN & '.'	Yes	Cart001	As provided in the request.
pp_ResponseCode	3 AN	Yes	000	Response code representing the transaction success or failure. A response code of 000 represents success. For a complete list of response codes refer to Appendix I.
pp_TokenizedCardNumber	16 N	No	91136333 78227378	This parameter can be accessible from 1.2 version. There are two types of tokenized card number in response. 1) The same Tokenized card number as received in request for returning customer 2)When customer selects save card option on Payment Portal Screen then PG returns a new tokenized card number in this field
pp_TokenizationResponseCode	3 AN	No	T00	This parameter can be accessible from 1.2 version. After save card details merchant will provide 3 digits response code to inform the status of tokenization. This field will be helpful for merchant to manage tokenized card against register customers.
pp_TokenizationResponseMsg	300 A	No	The tokenization operation was successfully processed	This parameter can be accessible from 1.2 version. After save card details merchant will provide a response message with respective to the pp_TokenizationResponseCode field as define above. This field will be mandatory for all cases where pp_TokenizationResponseCode is not equal to T00.
pp_CustomerCardNo	16 N	No	512345*** ***2346	This parameter can be accessible from 1.2 version.

				This field represents the masked card number of the customer against tokenized card.
pp_CustomerCardExpiry	4 N	Yes	0220	<p>This parameter can be accessible from 1.2 version.</p> <p>This field represents the customer card expiry against tokenized card. Example :</p> <p>0220 = February 2020</p>
pp_ResponseMessage	200 AN	No	Not enough balance to perform transaction	<p>Error details in case the transaction failed to be processed.</p> <p>This field will be mandatory for all cases where response code is not equal to 000.</p>
pp_RetrievalReferenceNo	12 N	No	000112233445	<p>A unique number generated by the Payment Gateway when the transaction got processed. The number should be stored and used for future reference.</p> <p>The number is unique for any given date.</p>
pp_AuthCode	12 N	No	123456	<p>An identifying code issued by the issuing bank to approve or deny the transaction.</p> <p>The field is mandatory in case of successful response code. Refer to Appendix I for a list of response codes and the codes which when sent will require Auth Code.</p>
pp_SettlementExpiry	14N	No	9 th Oct, 2011 10:35:47 PM will be sent as '2011009223547'	<p>A date supplied by the Payment Gateway indicating that if the merchant does not send a Confirmation of the transaction by this time, the PG will mark the transaction as expired and the Merchant will not be able to resume it.</p> <p>The field is mandatory in case of successful response code and when the AuthCode is not blank.</p>
pp_BankID	4 AN	Yes	BNK1	Customer's bank that authorized the transaction.

pp_ProductID	4 A	No	RETL	<p>This field will only be used in case of DD transaction type. Product of Bank through which payment has been performed. For e.g. Retail, Corporate.</p> <p>Fixed values: 'RETL', 'CORP'</p> <p>In case value was provided at the time of request, this field will contain the same value. Otherwise, ID of the product chosen by customer at PG will be filled.</p>
pp_SecureHash	64 AN	No	9e107d9d 372bb682 6bd81d35 42a419d6 9e107d9d 372bb682 6bd81d35 42a419d6	Used to allow the Merchant to check the integrity of the transaction response.
ppmpf_xxxx	255 AN	No		<p>Optional Fields</p> <p>Merchant can send additional information to PG in these fields while making the payment request. If received, the fields will be echoed back at the time of response.</p>
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		<p>Optional Fields</p> <p>Member Bank may send some additional information to Merchant.</p>
ppmbf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		

ppmbf_xxxx	255 AN	No		If received from Member Bank, PG will forward the information contained in this field to Merchant.
ppmbf_xxxx	255 AN	No		

6.2.3 Version 2.0

This version is used to support payment with tokenized approach. In this approach token will share with merchant through token generation notification.

Parameter	Max. Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.1	As provided in the request.
pp_TxnType	10 AN	No	PAY	As provided in the request.
pp_IsregisteredCustomer	3 A	Yes	Yes/No	As provided in the request.
pp_Language	3 A	Yes	EN	As provided in the request.
pp_MerchantID	10 AN	Yes	MERC001	Unique Id assigned to each Merchant by PG.
pp_SubMerchantId	10 AN	No	SUBMER001	As provided in the request.
pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx2011090901	As provided in the request.
pp_Amount	13 N	Yes	100.00 will be passed as 10000	If merchant wish to use discount module than final amount will be respond back which payaxis considers, else same amount will be responded as in the request.
pp_TxnCurrency	3 A	Yes	PKR	As provided in the request.
pp_TxnDateTime	14 N	Yes	9 th Sept, 2011 10:35:47 PM will be sent as '20110909203547'	As provided in the request.
pp_BillReference	20 AN & '.'	Yes	Cart001	As provided in the request.
pp_ResponseCode	3 AN	Yes	000	Response code representing the transaction success or failure. A response code of 000 represents success. For a complete list of

				response codes refer to Appendix I.
pp_TokenizedCardNumber	16 N	No	91136333 78227378	<p>This parameter can be accessible from 1.2 version. There are two types of tokenized card number in response.</p> <p>1) The same Tokenized card number as received in request for returning customer</p> <p>2) When customer selects save card option on Payment Portal Screen then PG returns a new tokenized card number in this field</p>
pp_TokenizationResponseCode	3 AN	No	T00	<p>This parameter can be accessible from 1.2 version.</p> <p>After save card details merchant will provide 3 digits response code to inform the status of tokenization.</p> <p>This field will be helpful for merchant to manage tokenized card against register customers.</p>
pp_TokenizationResponseMsg	300 A	No	The tokenization operation was successfully processed	<p>This parameter can be accessible from 1.2 version.</p> <p>After save card details merchant will provide a response message with respect to the pp_TokenizationResponseCode field as define above.</p> <p>This field will be mandatory for all cases where pp_TokenizationResponseCode is not equal to T00.</p>
pp_CustomerCardNo	16 N	No	512345*** ***2346	<p>This parameter can be accessible from 1.2 version.</p> <p>This field represents the masked card number of the customer against tokenized card.</p>
pp_CustomerCardExpiry	4 N	Yes	0220	This parameter can be accessible from 1.2 version.

				<p>This field represents the customer card expiry against tokenized card. Example :</p> <p>0220 = Feburay 2020</p>
pp_ResponseMessage	200 AN	No	Not enough balance to perform transaction	<p>Error details in case the transaction failed to be processed. This field will be mandatory for all cases where response code is not equal to 000.</p>
pp_RetreivalReferenceNo	12 N	No	000112233445	<p>A unique number generated by the Payment Gateway when the transaction got processed. The number should be stored and used for future reference. The number is unique for any given date.</p>
pp_AuthCode	12 N	No	123456	<p>An identifying code issued by the issuing bank to approve or deny the transaction.</p> <p>The field is mandatory in case of successful response code. Refer to Appendix I for a list of response codes and the codes which when sent will require Auth Code.</p>
pp_SettlementExpiry	14N	No	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	<p>A date supplied by the Payment Gateway indicating that if the merchant does not send a Confirmation of the transaction by this time, the PG will mark the transaction as expired and the Merchant will not be able to resume it.</p> <p>The field is mandatory in case of successful response code and when the AuthCode is not blank.</p>
pp_BankID	4 AN	Yes	BNK1	<p>Customer's bank that authorized the transaction.</p>
pp_ProductID	4 A	No	RETL	<p>This field will only be used in case of DD transaction type. Product of Bank through which payment has been performed. For e.g. Retail, Corporate.</p> <p>Fixed values: 'RETL', 'CORP'</p>

				In case value was provided at the time of request, this field will contain the same value. Otherwise, ID of the product chosen by customer at PG will be filled.
pp_SecureHash	64 AN	No	9e107d9d 372bb682 6bd81d35 42a419d6 9e107d9d 372bb682 6bd81d35 42a419d6	Used to allow the Merchant to check the integrity of the transaction response.
pp_CustomerID	255 AN	No	(Provided by Merchant)	As provided in the request.
pp_CustomerEmail	255 AN and !#\$%&*+ /=?^_`{ }~	No	sample@gmail.com	As provided in the request.
pp_CustomerMobile	11 N	No	03001237 896	As provided in the request
ppmpf_xxxx	255 AN	No		Optional Fields Merchant can send additional information to PG in these fields while making the payment request. If received, the fields will be echoed back at the time of response.
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmpf_xxxx	255 AN	No		
ppmbf_xxxx	255 AN	No		Optional Fields
ppmbf_xxxx	255 AN	No		

ppmbf_xxxx	255 AN	No		Member Bank may send some additional information to Merchant.
ppmbf_xxxx	255 AN	No		If received from Member Bank, PG will forward the information contained in this field to Merchant.
ppmbf_xxxx	255 AN	No		

6.2.4 Optional fields

The optional fields provided as part of the request will be returned to the merchant with the response, using the same parameter name as those provided by the merchant.

6.2.5 Optional Fields from Member Bank

Member Bank may forward some specific information to Merchant. To facilitate this operation PG Payment Portal also supports up to 5 member bank defined fields that will be sent from Member Bank to PG and PG Payment Portal will forward the optional fields to Merchant as part of the response.

These fields must be less than 255 bytes and must start with ppmbf_. These optional fields, if sent, will be part of the secure hash.

These fields are only forwarded in case of Direct Debit transactions. In case of Debit Card based transactions, these fields will be ignored.

6.3 Receiving the Transaction Response

To receive the transaction response, merchant must specify a return Internet address (return /URL). This address is also where the cardholder is returned to when they have completed the purchase. The pp_ReturnURL field must contain a valid URL (starting with "<http://>" or "<https://>") for every transaction request. If the ReturnURL value does not form a valid URL, an error is generated in the Payment Server which will stop the transaction. Moreover, the starting of the URL should be provided to PMCL before transaction processing can begin. The pp_ReturnURL field is validated against this part URL for security puposes. If the values do not match, transaction is rejected.

7. Payment Status Inquiry

In addition to performing payments using the PG Payment Portal, the merchant can also inquire the status of any transaction using the Payment Status Inquiry Web Service should it fail to receive any response from Payment Gateway within a particular interval.

The Payment Status Inquiry service allows merchant to check the status of any transaction it has performed through the Payment Gateway. The inquiry will in turn respond with the transaction status (success or failure or pending) along with error message, if applicable.

7.1 Payment Status Inquiry Input Parameters

The signature of Payment Status Inquiry Web Service which the merchant may call to fetch transaction status is:

TestURL:

http://119.160.80.70/ExternalStatusService/StatusService_v11.svc?wsdl

```
Public string DoPaymentStatusInquiryNew(string pp_Version, string pp_TxnType, string pp_MerchantId, string pp_Password, string pp_TxnRefNo, string pp_TxnDateTime, string pp_SecureHash)
```

The parameter names and details of each parameter are described below:

Parameter	Max. Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.1	Payment Portal Version. Fixed value '1.1' should be used
pp_TxnType	10 AN	No	PAY	Presents the transaction type: <ul style="list-style-type: none"> Transactions via Internet Banking = DD Mobile Wallet = MWALLET Master Card = MIGS Over The Counter = OTC Debit Card = PAY
pp_Merchant ID	10 AN	Yes	MERC001	Unique Id assigned to each Merchant by PG.
pp_Password	10 AN	Yes	75019F19EA	Password is assigned to each merchant and is used to authenticate merchant at the time of payment. Password is a system generated value.

pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx2011090901	As provided in the transaction processing request.
pp_TxnDateTime	14 N	Yes	9th Sept, 2011 10:35:47 PM will be sent as '20110909203547'	The transaction date time that was provided at the time of transaction execution.
pp_SecureHash	64 AN	No	9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6	Used to allow the Payment Gateway to check the integrity of the transaction response.

7.2 Payment Status Inquiry Response

In response to the above stated function call, the Payment Status Inquiry will respond with a string which will contain the response code, followed by other transaction authorization related fields as provided in the Payment Portal Transaction Processing response. Also, the response sent will be fixed length and white spaces will be padded with the ASCII:32 if parameter is left as empty

Parameter	Max. Length	Mandatory	Sample Values	Remarks
Response Code	3 AN	Yes	000	First three characters of the string denoting the response code. For list of response codes see Appendix I.
Response Message	200 AN	No	Low Balance	The Response Message field shows message corresponding to the response code. It is concatenated with the response code. In case Response code is '000' i.e. Success, this field will be all spaces. This field will be mandatory for all cases where response code is not equal to 000.
Retrieval Reference No	12 N	Yes	000112233445	A unique number generated by the Payment Gateway at the time of transaction processing. The number should be stored and used for future reference. The number is unique for any given date.

Settlement Date	8 N	No	For 9th Sept, 2011 value will be 20110909	<p>A date supplied by the Payment Gateway to indicate when this transaction will be settled.</p> <p>When the Payment Gateway closes the batch at the end of the day, the date will roll over to the next processing day's date. This date will only be provided in case a transaction is already confirmed by the merchant.</p>
Auth Code	12 N	No	123456987456	<p>An identifying code issued by the issuing bank to approve or deny the transaction.</p> <p>The field is mandatory in case of successful response code. Refer to Appendix I for a list of response codes and the codes which when sent will require Auth Code.</p>
Settlement Expiry	14N	No	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223 547'	<p>A date supplied by the Payment Gateway indicating that if the merchant does not send a Confirmation of the transaction by this time, the PG will mark the transaction as expired and the Merchant will not be able to resume it.</p> <p>This field will be mandatory where Auth Code is available.</p>
BankID	4 AN	No	BNK1	<p>This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field.</p> <p>Customer's bank that authorized the transaction.</p>
ProductID	4 A	No	RETL	<p>This field will only be used in case of DD transaction type. Product of Bank through which payment has been performed. For e.g. Retail, Corporate.</p> <p>Fixed values: 'RETL', 'CORP'</p> <p>In case value was provided at the time of request, this field will contain the same value. Otherwise, ID of the product chosen by customer at PG will be filled.</p>

CustomerCardNo	20 N	No	987156324000 123654789	As provided in the transaction cycle. This field will only be sent as empty if the transaction type is OTC/MIGS/Mwallet.
Secure Hash	64 AN	No	9e107d9d372b b6826bd81d35 42a419d69e10 7d9d372bb682 6bd81d3542a4 19d6	Used to allow the Merchant to check the integrity of the transaction request.

7.3 Payment Status Inquiry Processing

- On receiving the request from Merchant, Payment Gateway will check whether it has the transaction in pending state or not.
- If the transaction is NOT in pending state, that is, the transaction is either in Success/Approved or Failed/Denied/Expired stage, the same response will be sent to Merchant. In case of Approved transaction, Settlement Expiry will be sent as well. Note that the Settlement Expiry is calculated at the time the approval of transaction was received from the bank and not when the inquiry request was received.
- In case of Pending transaction, PG will proceed to inquire the status of the transaction. This status can occur at over the counter transaction.
- If inquiry is initiated after Settlement Expiry or Transaction Expiry has elapsed, a response code indicating the same would be sent to Merchant.
- Merchant may not receive the response to a Status Inquiry call. This can happen in following scenario(s):
 - The response PG sends to the Merchant is lost due to network problems.

In the above case, Merchant will need to send the inquiry again to get the status.

8. Payment Status Update

Merchant will be required to expose a transaction status update web service for Payment Gateway to update status of transactions which are not executed instantaneously.

There is a possibility that at the time of voucher transaction creation, the transaction is not executed right away but requires certain procedure to actually processed. This is a common scenario for voucher based transactions. In such cases, when Payment Gateway generates the voucher, customer has to visit the JazzCash outlet for the payment of voucher, Payment Gateway will in turn call the merchant Status update web service to update the status at merchant's end against the voucher number.

8.1 Update Payment Status Input Parameters

The signature of Payment Status Update Web Service which the Payment Gateway will call to update transaction status is:

The parameter names and details of each parameter are described below:

Parameter	Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.1	Payment Portal Version. Fixed value '1.1' should be used
pp_TxnType	10 AN	Yes	OTC	Presents the transaction type: <ul style="list-style-type: none"> Transactions via Internet Banking = DD Over The Counter = OTC Mobile Wallet = MWALLET Card based = MIGS
pp_BankID	4AN	No	BNK1	Bank Id of the bank that has authorized the transaction. This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field.
pp_ProductID	4 A	No	RETL	This field will only be used in case of DD transaction type. Product of Bank through which payment has been performed. For e.g. Retail, Corporate. Fixed values: 'RETL', 'CORP' In case value was provided at the time of request, this field will contain the same value. Otherwise, ID of the product chosen by customer at PG will be filled.
pp_Password	10 AN	Yes	75019F19EA	Password is assigned to each merchant and can be used by the Merchant to identify if the transaction is coming from PG or not.
pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx2011090901	As provided in the transaction processing request.

pp_TxnDateTime	14 N	Yes	9th Sept, 2011 10:35:47 PM will be sent as '20110909203547'	The transaction date time that was provided at the time of transaction execution.
pp_ResponseCode	3 AN	Yes	000	Response Code signifies the transaction execution status as received from the Bank. For complete details of possible response codes see Appendix I.
pp_ResponseMessage	200 AN	No	Low Balance	The Response Message field shows message corresponding to the response code. It is concatenated with the response code. In case Response code is '000' i.e. Success, this field will be all spaces. This field will be mandatory for all cases where response code is not equal to 000.
pp_AuthCode	12 N	No	123456	An identifying code issued by the issuing bank to approve or deny the transaction. This will be mandatory for successfully authorized transactions.
pp_SettlementExpiry	14N	No	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	A date supplied by the Payment Gateway indicating that if the merchant does not send a Confirmation of the transaction by this time, the PG will mark the transaction as expired and the Merchant will not be able to resume it. This will be mandatory for successfully authorized transactions.
pp_RetrievalReferenceNo	12 N	Yes	000112233445	A unique number generated by the Payment Gateway at the time of transaction processing. The number may be stored and used for future reference. The number is unique for any given date.
pp_SecureHash	64 AN	No	9e107d9d372bb682 6bd81d3542a419d6 9e107d9d372bb682 6bd81d3542a419d6	Used to allow the Merchant to check the integrity of the transaction message.

8.2 Update Payment Status Response

In response to the above stated function call, the merchant will respond with a string which will contain the response code and error message if any.

Parameter	Length	Mandatory	Sample Values	Remarks
Response Code	3 AN	Yes	000	First three characters of the string denoting the response code. For list of response codes see Appendix I.
Response Message	200 AN	No	Invalid Secure Hash	The Response Message field shows message corresponding to the response code. It is concatenated with the response code. In case Response code is '000' i.e. Success, this field will be empty. This field will be mandatory for all cases where response code is not equal to 000.
Secure Hash	64 AN	No	9e107d9d372b b6826bd81d35 42a419d69e10 7d9d372bb682 6bd81d3542a4 19d6	Used to allow the Payment Gateway to check the integrity of the transaction request.

8.3 Update Payment Status Reiteration

In cases when the Payment Status update service response is not received by the Payment Gateway application on initial request (implying network glitches during the service calling or receiving response), the update service will be invoked again for updating the payment status on the merchant. Payment Gateway will continue invoking the service for a configurable number of times until the response is received.

At the Merchant end if the update service is called for the payment which is already updated, only an acknowledgment response should be sent even if the response was sent earlier.

After retries have been exhausted Payment Gateway will stop sending update request to Merchant. In case merchant needs to know the status of a transaction, it may invoke Payment Gateway's inquiry service.

9. Delivery Status Update

After a transaction has completed its span at Merchant's end, Merchant will need to send a confirmation to Payment Gateway. This confirmation message should be sent in the following scenarios:

1. Transaction has completed successfully and delivery has been made to the customer.
2. Goods or service could not be delivered to the customer for any reason.

In case a confirmation message of successful transaction is received by PG, the transaction will be marked completed and settlement of the same transaction will be done at PG's end.

In case confirmation message of reverse transaction is received by PG, the transaction will be marked 'Awaiting Reversal' and reversal for the same transaction will be initiated to the bank. PG will then send a reversal transaction to bank. On receiving success response from bank the transaction's status will be updated to 'Reverse'.

9.1 Delivery Status Update Input Parameters

The signature of Delivery status update web service which the Merchant will call to confirm transaction's completion is:

```
public string DoUpdateDeliveryStatus(string pp_Version, string pp_TxnType, string pp_DeliveryStatus, string pp_MerchantId, string pp_Password, string pp_TxnRefNo, string pp_TxnDateTime, string pp_SecureHash)
```

The parameter names and details of each parameter are described below:

Parameter	Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.1	Payment Portal Version. Fixed value '1.1' should be used
pp_TxnType	10 AN	No	PAY	Presents the transaction type: <ul style="list-style-type: none"> Transactions via Internet Banking = DD Mobile Wallet = MWALLET Master Card = MIGS Over The Counter = OTC Debit Card = PAY
pp_DeliveryStatus	3 AN	Yes	CFM	Possible values: 'CFM': to indicate confirmation, 'REV': to indicate reversal and void

pp_MerchantID	10AN	No	MERC001	Id of Merchant initiating the request and which initiated the transaction
pp_Password	10 AN	Yes	75019F19EA	Password is assigned to each merchant and will be used by the PG to identify if the transaction is from a valid merchant.
pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx2011090901	As provided in the transaction processing request.
pp_TxnDateTime	14 N	Yes	9th Sept, 2011 10:35:47 PM will be sent as '20110909203547'	The transaction date time that was provided at the time of transaction execution
pp_SecureHash	64 AN	No	9e107d9d372bb682 6bd81d3542a419d6 9e107d9d372bb682 6bd81d3542a419d6	Used to allow the Payment Gateway to check the integrity of the transaction request.

9.2 Delivery Status Update Response Parameters

In response to the above stated function call, Payment Gateway will respond with a string which will contain the response code and error message if any.

Parameter	Length	Mandatory	Sample Values	Remarks
Response Code	3 AN	Yes	000	First three characters of the string denoting the response code. This response indicates the success or failure of delivery status update request sent by the merchant rather than the status of the actual transaction. For list of response codes see Appendix I.
Response Message	200 AN	No	Transaction Expired	The Response Message field shows message corresponding to the response code. It is concatenated with the response code. In case Response code is '000' i.e. Success, this field will be all spaces. This field will be mandatory for all cases where response code is not equal to 000.
Settlement Date	8 N	No	For 9th Sept, 2011 value will be 20110909	A date supplied by the Payment Gateway to indicate when this transaction will be settled.

				When the Payment Gateway closes the batch at the end of the day, the date will roll over to the next processing day's date. This date will only be provided in response to a transaction confirmation by the merchant.
Secure Hash	64 AN	No	9e107d9d372b b6826bd81d35 42a419d69e10 7d9d372bb682 6bd81d3542a4	Used to allow the Merchant to check the integrity of the response.

9.3 Delivery Status Update Processing

- Merchants will use the Status Update web service to provide the updated status of the transactions to PG. Merchant will be using Status Update Service in following scenarios
 - To provide the confirmation of approved transactions to PG.
 - Request to Reverse the transaction after receiving an approval from PG.
 - Request to VOID the transaction which is in Pending state.
- If PG receives an inquiry or status update after receiving a Reversal or Void request from merchant, a response stating that transaction has been marked as Reserved or Void will be sent to merchant

To provide the confirmation of approved transactions to PG

- On receiving an approval of pending transaction from Payment Gateway, Merchant will process and update the status of transaction at its end and once successfully done, will provide the confirmation to Payment Gateway.
 - PG will entertain the confirmation message only for those transactions which are already Approved and the confirmation is received within Settlement Expiry period.
- On receiving confirmation from Merchant, Payment Gateway will mark the transaction as 'Confirmed'.
 - If for any reason, Merchant is not able to complete a transaction within Settlement expiry span, Merchant may send a request to reverse the transaction. PG will entertain this message only for transactions that are already approved and lie within the settlement expiry. After checking the status of transaction, PG will mark the transaction as Reversed in its database and will update accordingly.

Request to VOID the transaction which is in Pending State

- If Merchant would like to VOID the transaction which is in “Pending State” and lie within the transaction expiry, Merchant may send a request to VOID the transaction to PG. After checking the status of transaction, PG will mark the transaction as VOID in its database and will update accordingly.

For reference, consider the below table which indicates the response that will be sent to Merchant in case the transaction is in the mentioned status:

Transaction Status	Response Returned
Awaiting Reversal	Delivery Status cannot be updated
Reversal	Delivery Status cannot be updated
Awaiting Void	Delivery Status cannot be updated
Void	Delivery Status cannot be updated
Success	Respective code
Failed	Delivery Status cannot be updated
Pending	Successful (000) in case of REV, Delivery Status cannot be updated in case of CFM
Confirmed	Delivery Status cannot be updated
Expired	Delivery Status cannot be updated

10. Refund Transaction

Transaction performed using Debit Card can be refunded only.

In the event of a customer dispute the merchant may need to make full refund of transaction. The transaction refund option will allow the merchant to refund a transaction processed by the Payment Gateway.

This option will be available in the Merchant Portal. Further details of this feature can be found in the Merchant Portal User Guide.

11. Integration with PG Via Payment API

For merchants to enable payment through Payment Gateway, they are required to consume payment API. This section describes in detail how to integrate the merchant e-commerce website with the PG Payment API.

Merchant will provide the input parameters using SOAP request to the PG Payment API. The PG Payment API will process transaction and return the response via SOAP message. The merchant may use the response to show the transaction results (success or failure) of the transaction to the customer.

11.1 Payment API - Input Parameters

To integrate with Payment Gateway through Payment API, a wsdl file will be shared to merchant. Merchant will use the provided WSDL and

access below Test URL to consume this API on merchant website. Transaction request format is discussed below in detail.

TestURL:

http://119.160.80.70/ExternalStatusService/StatusService_v11.svc?wsdl

```
public string DoPaymentViaAPI(string pp_Version, string pp_TxnType,
string pp_Language, string pp_MerchantID, string pp_SubMerchantID,
string pp_Password, string pp_BankID, string pp_ProductID, string
pp_TxnRefNo, string pp_Amount, string pp_TxnCurrency, string
pp_TxnDateTime, string pp_BillReference, string pp_Description, string
pp_TxnExpiryDateTime, string pp_ReturnURL, string pp_SecureHash, string
ppmpf_1, string ppmpf_2, string ppmpf_3, string ppmpf_4, string ppmpf_5)
```

This API will receive a SOAP request from the merchant website which will contain the merchant authentication details along with the transaction details. The Payment API will validate and process the transaction. The request will be containing the input parameters as

Note : Sample xml request is provided in the end of this section.

11.2 Payment API - Request Parameters

The PG Payment API will receive a SOAP request from the merchant website which will contain the merchant authentication details along with the transaction details. The Payment API will validate and process the transaction. The request will be containing the input parameters as XML fields as:

Parameter	Max. Length	Mandatory	Sample Values	Remarks
pp_Version	4 AN	Yes	1.1	Payment Portal Version. Fixed value '1.1' should be used
pp_TxnType	10 AN	Yes	OTC or MWALLET	Presents the transaction type: Over The Counter = OTC, Mobile Account = MWALLET
pp_Language	3 A	Yes	EN	Specifies the language in which to display the page. Fixed value 'EN'.
pp_MerchantID	10 AN	Yes	MERC001	Unique Id assigned to each Merchant by PG.
pp_SubMerchantID	10 AN	No	SUBMER001	If the merchant is handling any child merchants at its end, then the child merchant Id will be

				provided. The Transaction reports will be grouped on the basis of Sub Merchant Id, if available.
pp_Password	10 AN	Yes	75019F19EA	Password is assigned to each merchant and is used to authenticate merchant at the time of payment. Password is a system generated value.
pp_BankID	4AN	No	BNK01	This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field. Bank Id of the customer's banks if available.
pp_ProductID	4 A	No	RETL	This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field. Product of Bank through which payment will be done. For e.g. Retail, Corporate. Fixed values: 'RETL', 'CORP'
pp_TxnRefNo	20 AN & '/' & '.'	Yes	Tx2011090901	A unique value created by the merchant to identify the transaction.
pp_Amount	13 N	Yes	100.00 will be passed as 10000	The transaction amount. Please note that no decimal places are included. Decimal place will be assumed at the default position of the currency provided.
pp_TxnCurrency	3 A	Yes	PKR	Currency of Transaction amount. It has a fixed value 'PKR'.
pp_TxnDateTime	14 N	Yes	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	Merchant provided date and time of transaction. The format of date time should be yyyyMMddHHmmss.
pp_BillReference	20 AN & '.'	Yes	Cart001	Bill/invoice Number being settled.
pp_Description	200 Free Text Field	Yes	Payment for 3 Item(s) bought	Transaction details to be shown on screen as desired by the merchant. This field will be parsed to identify any malicious data entered by the end user. In cases when any of these characters <>*=%/:"{} are inserted, they will be replaced with a space. Pipe ' ' is not allowed

pp_TxnExpiryDate	14 N	Yes	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	Transaction Expiry can be specified by merchant to indicate to the issuing bank that the transaction must be approved within this period. Please note that the default and maximum value of this expiry is 3 months.
pp_ReturnURL	200 AN	Yes	Merchant site/payment/Results.aspx	This field is mandatory and merchant must share this URL before using API as it will be a part of merchant profile. URL should always be the same in every request once shared. It is a part of merchant authentication, difference of URL will fail the validation.
pp_SecureHash	64 AN	No	9e107d9d372bb682 6bd81d3542a419d6 9e107d9d372bb682 6bd81d3542a419d6	Used to allow the Payment Gateway to check the integrity of the transaction request.
ppmpf_1	255 AN	Yes	03211234567	Mobile Number Field
ppmpf_2	255 AN	No	100.00 will be passed as 10000	Discounted Amount
ppmpf_3	255 AN	No	SCB	Discount bank
ppmpf_4	255 AN	No		Optional Fields
ppmpf_5	255 AN	No		Merchant can send additional information to PG in this field. These will be returned to Merchant in transaction response. xxxx in the name for Optional fields can be replaced by any set of characters.

11.2.1 Optional Merchant Defined Fields

Payment Gateway API also supports up to 4 merchant defined fields that will be returned to the merchant in transaction response.

These fields must be less than or equal to 255 bytes and These fields will only be exchanged during SOAP request/response.

11.3 Payment API Response

The response by Payment Gateway Payment API will send the transaction results to the merchant portal so that the merchant can perform the required operations accordingly.

The details will be sent against the request initiated by merchant using SOAP Payment API. The response parameters returned by the Payment Portal are described below.

SOAP response will be sent to merchant in an alphabetical order separated by pipe '|'. Merchant need to parse the response and show the transaction results to user on any screen accordingly. Response parameter detail with sequence number is as follows.

Parameter	Max. Length	Mandatory	Sequence	Sample Values	Remarks
pp_Version	4 AN	Yes	17	1.1	As provided in the request.
pp_TxnType	10 AN	No	16	PAY	As provided in the request.
pp_Language	3 A	Yes	5	EN	As provided in the request.
pp_MerchantID	10 AN	Yes	6	MERC001	Unique Id assigned to each Merchant by PG.
pp_SubMerchantId	10 AN	No	12	SUBMER001	As provided in the request.
pp_TxnRefNo	20 AN & '/' & '.'	Yes	15	Tx2011090901	As provided in the request.
pp_Amount	13 N	Yes	1	100.00 will be passed as 10000	If merchant wish to use discount module than final amount will be respond back which payaxis considers, else same amount will be responded as in the request.
pp_TxnCurrency	3 A	Yes	13	PKR	As provided in the request.
pp_TxnDateTime	14 N	Yes	14	9 th Sept, 2011 10:35:47 PM will be sent as '20110909203547'	As provided in the request.
pp_BillReference	20 AN & '.'	Yes	4	Cart001	As provided in the request.
pp_ResponseCode	3 AN	Yes	7	000	Response code representing the transaction success or failure. A response code of 000 represents success. For a complete list of response codes refer to Appendix I.
pp_ResponseMessage	200 AN	No	8	Not enough balance to perform transaction	Error details in case the transaction failed to be processed.

					This field will be mandatory for all cases where response code is not equal to 000.
pp_RetreivalReferenceNo	12 N	Yes	9	000112233445	A unique number generated by the Payment Gateway at the time of transaction processing. The number should be stored and used for future reference. The number is unique for any given date.
pp_AuthCode	12 N	No	2	123456	An identifying code issued by the issuing bank to approve or deny the transaction. The field is mandatory in case of successful response code. Refer to Appendix I for a list of response codes and the codes which when sent will require Auth Code.
pp_SettlementExpiry	14N	No	11	9 th Oct, 2011 10:35:47 PM will be sent as '20111009223547'	A date supplied by the Payment Gateway indicating that if the merchant does not send a Confirmation of the transaction by this time, the PG will mark the transaction as expired and the Merchant will not be able to resume it. The field is mandatory in case of successful response code and when the AuthCode is not blank.
pp_BankID	4 AN	Yes	3	BNK1	Customer's bank that authorized the transaction.
pp_SecureHash	64 AN	No	10	9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6	Used to allow the Merchant to check the integrity of the transaction response.
ppmbf_xxxx	255 AN	No	18	Optional Fields Merchant may send some additional information to Member Bank. If received, PG will forward the information contained in this field to bank. xxxx in the name for Optional fields can be replaced by any set of characters.	
ppmbf_xxxx	255 AN	No	19		
ppmbf_xxxx	255 AN	No	20		

ppmbf_xxxx	255 AN	No	21		
ppmbf_xxxx	255 AN	No	22		
ppmpf_1	255 AN	Yes	23	03211234567	Mobile Number Field Format : xxxxxxxxxxxx
ppmpf_2	255 AN	No	24		Optional Field Merchant can send additional information to PG in this field while making the payment request. If received, the fields will be echoed back at the time of response.
ppmpf_3	255 AN	No	25		
ppmpf_4	255 AN	No	26		
ppmpf_5	255 AN	No	27		

11.3.1 Optional fields

The optional fields provided as part of the request will be returned to the merchant with the response, using the same parameter name as those provided by the merchant.

11.3.2 Receiving Payment API Response

Success response code for OTC is “124 : Your order is placed and waiting for financials to be received “ whereas success response code for MWALLET is “000” ,for other response code please refer 14 Appendix 1- Repsonse Code section below.

Please Note: Return URL field in payment API is only a part of merchant authentication and should be same in every transaction request once provided by merchant, merchant will parse the response received from Payment Gateway and is allowed to display on any merchant screen as per convenience.

11.4 Sample API Requests

11.4.1 Sample Payment API Request from SOAP UI Tool

```

<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tem="http://tempuri.org/"
<soapenv:Header/>
<soapenv:Body>
  <tem:DoPaymentViaAPI>

    <tem:pp_Version>1.1</tem:pp_Version>
    <tem:pp_TxnType>OTC</tem:pp_TxnType>
    <tem:pp_Language>EN</tem:pp_Language>
    <tem:pp_MerchantID>TestMerc0003</tem:pp_MerchantID>
    <tem:pp_SubMerchantID/>
    <tem:pp_Password>0123456789</tem:pp_Password>
    <tem:pp_BankID/>
    <tem:pp_ProductID/>

    <tem:pp_TxnRefNo>TR160825173822</tem:pp_TxnRefNo>
    <tem:pp_Amount>10000</tem:pp_Amount>
    <tem:pp_TxnCurrency>PKR</tem:pp_TxnCurrency>
    <tem:pp_TxnDateTime>20160825174445</tem:pp_TxnDateTime>
    <tem:pp_BillReference>0123456</tem:pp_BillReference>
    <tem:pp_Description>Product</tem:pp_Description>

    <tem:pp_TxnExpiryDateTime>20160830113600</tem:pp_TxnExpi
ryDateTime>
    <tem:pp_ReturnURL>http://localhost/MerchantSimulator/HttpR
equestDemoServer/Index</tem:pp_ReturnURL>
    <tem:pp_SecureHash>5212E6DC8A73E6335663476E9A52CEF99508
11815529E8C2F44F7125D0B3E3E2</tem:pp_SecureHash>
      <tem:ppmpf_1>03312456985</tem:ppmpf_1>
      <tem:ppmpf_2>2</tem:ppmpf_2>
      <tem:ppmpf_3>3</tem:ppmpf_3>
      <tem:ppmpf_4>4</tem:ppmpf_4>
      <tem:ppmpf_5>5</tem:ppmpf_5>

    </tem:DoPaymentViaAPI>
  </soapenv:Body>
</soapenv:Envelope>

```

11.4.2 Sample Payment API Response

SOAP sample response in an alphabetical order separated by pipe '|'. Parse the data according to the response sequence guid provided above.

Response![10000|||0123456|EN|MERC0003|124|Order is placed and waiting for financials to be received over the counter.|160825002328|4551BFAF3332B2A7712CD4EFFD36396E5CC8B4ED9A3C2CAFA7324C1FD9C8E769|||PKR|20160825174445|TR160825173822|OTC|1.1|||03312456985]

Note : Consider the value empty between two PIPs'|' if no value is present.

eg : 10000|||0123456

12. Integration with Card payment - API

For merchants to enable payment processing of debit/ credit card through Payment Gateway's API, they are required to integrate with the Payment Gateway API. This section describes in detail how to integrate the merchant e-commerce website with the PG Payment API to perform card payments.

Merchant is required to integrate the PG payment REST based APIs. The PG payment portal will process the transaction and return the response which merchant may use to show the transaction results (success or failure) of the transaction to the customer.

Merchant may integrate the API's provided below:

- Payment Authorize
- Payment Capture
- Payment Void
- Payment Refund
- Payment Retrieve
- Check 3DS enrollment
- Process ACS
- Payment Direct Pay

12.1 Payment Authorize - Request JSON

This is a request to obtain an authorization for a proposed funds transfer. An authorization is a response from a financial institution indicating that payment information is valid and funds are available in the payers account.

Version 1.1

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/api/authorize/AuthorizePayment
Production URL	Will be communicated after business approval

Headers	application/json
Body	<pre>{ "AuthorizeRequest":{ "pp_InstrumentType":"CARD", "pp_TxnRefNo":"T20170425112425", "pp_Amount":"10000", "pp_TxnCurrency":"PKR", "InstrumentDTO":{ "pp_CustomerCardNumber":"4557012345678902", "pp_CustomerCardExpiry":"1020", "pp_CustomerCardCvv":"101" }, "pp_MerchantID":"Test00127801", "pp_Password":"000000000", "pp_SecureHash":"", "pp_Frequency": "SINGLE" } }</pre>

Version 2.0

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/api/2.0/authorize/AuthorizePayment
Production URL	Will be communicated after business approval
Headers	application/json

Body	<pre> { "pp_InstrumentType": "CARD", "pp_Frequency": "SINGLE", "pp_TxnRefNo": "T20190415174304", "pp_Amount": "20000", "pp_TxnCurrency": "PKR", "pp_CustomerCardNumber": "5123456789012346", "pp_CustomerCardExpiry": "0521", "pp_CustomerCardCw": "111", "pp_MerchantID": "Test00127801", "pp_Password": "000000000", "pp_CustomerID": "test", "pp_CustomerEmail": "test@test.com", "pp_CustomerMobile": "03222852628", "pp_SecureHash": "" } </pre>
-------------	---

12.2 Payment Authorize - Response JSON

Version 1.1

Body	<pre> { "responseCode": "", "responseMessage": "" } </pre>
-------------	--

Version 2.0

Body	<pre> { "pp_InstrToken": "", "pp_TokenizationResponseCode": "", "pp_TokenizationResponseMessage": "", "pp_CustomerCardNumber": "", "pp_CustomerCardExpiry": "", "pp_CustomerID": "", "pp_CustomerEmail": "" } </pre>
-------------	--

	<pre> "pp_CustomerMobile": "", "pp_ShouldTokenizeCardNumber": "", "pp_IsRegisteredCustomer": "", "pp_TxnRefNo": "", "pp_MerchantID": "", "pp_Password": "", "pp_Amount": "", "pp_TxnCurrency": "", "pp_InstrumentType": "", "pp_Frequency": "", "pp_3DSecureID": "", "pp_SecureHash": "", "pp_ResponseCode": "", "pp_ResponseMessage": "" } </pre>
--	--

12.3 Payment Authorize Via Token -Request JSON

This is a request to obtain an authorization for a proposed funds transfer. An authorization is a response from a financial institution indicating that payment information is valid and funds are available in the payers account.

Version 2.0

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/api/2.0/authorize/AuthorizePaymentViaToken
Production URL	Will be communicated after business approval
Headers	application/json

Body	<pre>{ "pp_InstrumentType": "CARD", "pp_Frequency": "SINGLE", "pp_IsRegisteredCustomer": "Yes", "pp_TxnRefNo": "T20190424102755", "pp_Amount": "100", "pp_TxnCurrency": "PKR", "pp_TokenizedCardNumber": "9475251683607119", "pp_MerchantID": "Test00127801", "pp_Password": "000000000", "pp_CustomerID": "", "pp_CustomerEmail": "", "pp_CustomerMobile": "", "pp_SecureHash": "" }</pre>
-------------	---

12.4 Payment Authorize Via Token-Response JSON

Version 2.0

Body	<pre>{ "pp_IsRegisteredCustomer": "", "pp_TxnRefNo": "", "pp_MerchantID": "", "pp_Password": "", "pp_Amount": "", "pp_TxnCurrency": "", "pp_InstrumentType": "", "pp_Frequency": "", "pp_3DSecureID": "", "pp_InstrToken": "", "pp_CustomerID": "", "pp_CustomerEmail": "", "pp_CustomerMobile": "", "pp_TokenizedCardNumber": "", "pp_SecureHash": "" }</pre>
-------------	--

	<pre>"pp_ResponseCode": "", "pp_ResponseMessage": "" }</pre>
--	--

12.5 Payment Capture -Request JSON

This is a request to capture funds previously reserved by an authorization. A Capture transaction triggers the movement of funds from the payer's account to the merchant's account.

Version 1.1

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/api/authorize/Capture
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre>{ "CaptureRequest": { "pp_TxnRefNo": "T20170425112425", "pp_Amount": "10000", "pp_TxnCurrency": "PKR", "pp_MerchantID": "Test00127801", "pp_Password": "0123456789", "pp_SecureHash": "" } }</pre>

Version 2.0

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/api/2.0/authorize/Capture
Production URL	Will be communicated after business approval
Headers	application/json

Body	<pre>{ "pp_TxnRefNo": "T20190415103607", "pp_Amount": "20000", "pp_TxnCurrency": "PKR", "pp_MerchantID": "Test00127801", "pp_Password": "0000000000", "pp_SecureHash": "" }</pre>
-------------	---

12.6 Payment Capture -Response JSON

Version 1.1

Body	<pre>{ "responseCode": "", "responseMessage": "" }</pre>
-------------	--

Version 2.0

Body	<pre>{ "pp_TxnRefNo": "", "pp_MerchantID": "", "pp_Password": "", "pp_Amount": "", "pp_TxnCurrency": "", "pp_3DSecureID": "", "pp_SecureHash": "", "pp_ResponseCode": "", "pp_ResponseMessage": "" }</pre>
-------------	--

12.7 Payment Void - Request JSON

This is a request to void a previous transaction. A void will reverse a previous transaction.

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/api/authorize/Void
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre>{ "VoidRequest": { "pp_TxnRefNo": "T20170425112425", "pp_MerchantID": "Test00127801", "pp_Password": "0123456789", "pp_SecureHash": "" } }</pre>

12.8 Payment Void - Response JSON

Body	<pre>{ "responseCode": "", "responseMessage": "" }</pre>
-------------	--

12.9 Payment Refund -Request JSON

This is a request to refund previously captured funds to the payer. Typically, a Refund is linked to the Capture or Pay through the txnrefno.

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/api/authorize/Refund
Production URL	Will be communicated after business approval
Headers	application/json

Body	<pre>{ "RefundRequest" : { "pp_TxnRefNo":"T20170425112424", "pp_Amount":"9999", "pp_TxnCurrency":"PKR", "pp_MerchantID":"Test00127801", "pp_Password":"0123456789", "pp_SecureHash":"" } }</pre>
-------------	--

12.10 Payment Refund -Response JSON

Body	<pre>{ "responseCode": "", "responseMessage": "" }</pre>
-------------	--

12.11 Payment Retrieve - Request JSON

This is a request retrieve the details of an order and all transactions associated with this order.

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/api/PaymentInquiry/Inquire
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre>{ "pp_TxnRefNo":"T20170518161115", "pp_MerchantID":"Test00127801", "pp_Password":"0123456789", "pp_SecureHash":""," "pp_Version":"1.1" }</pre>

12.12 Payment Retrieve - Response JSON

Body	<pre>{ "status": "", "rrn": "", "settlementDate": "", "settlementExpiryDate": "", "authCode": "", "bankID": "", "productID": "" }</pre>
-------------	---

12.13 Check 3DS enrollement - Request JSON

This is a request to check a cardholder's enrollment in the 3D Secure scheme.

Version 1.1

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/API/Purchase/Check3DsEnrollment
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre>{ "pp_Version": "1.1", "pp_TxnType": "MPAY", "pp_TxnRefNo": "T20170425112405", "pp_MerchantID": "Test00127801", "pp_Password": "0123456789", "pp_Amount": "20000", "pp_TxnCurrency": "PKR", "pp_TxnDateTime": "20170512101250", "pp_TxnExpiryDateTime": "20170514101250", "pp_BillReference": "billRef", "pp_Description": "Description of transaction", "pp_CustomerCardNumber": "5111111111111118", "pp_CustomerCardExpiry": "0517", "pp_CustomerCardCvv": "100", "pp_SecureHash": "" }</pre>

Version 2.0

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/API/2.0/Purchase/Check3DsEnrollment
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre>{ "pp_TxnType": "MPAY", "pp_TxnRefNo": "T20170425112405", "pp_MerchantID": "Test00127801", "pp_Password": "0123456789", "pp_Amount": "20000", "pp_TxnCurrency": "PKR", "pp_TxnDateTime": "20170512101250", "pp_TxnExpiryDateTime": "20170514101250", "pp_BillReference": "billRef", "pp_Description": "Description of transaction", "pp_CustomerCardNumber": "5111111111111118", "pp_CustomerCardExpiry": "0517", "pp_CustomerCardCvv": "100", "pp_IsRegisteredCustomer": "Yes", "pp_CustomerID": "test", "pp_CustomerEmail": "test@test.com", "pp_CustomerMobile": "033567890", "pp_SecureHash": "" }</pre>

12.14 Check 3DS enrollement - Response JSON

Version 1.1

Body	<pre>{ "result_CardEnrolled": "", "c3dSecureID": "", "aR_Simple_Html": "", "responseCode": "", "responseMessage": "" }</pre>
-------------	--

Version 2.0

Body	<pre> { "pp_IsRegisteredCustomer": "Yes", "summaryStatus": "CARD_ENROLLED", "pp_CustomerID": "test", "pp_CustomerEmail": "test@test.com", "pp_CustomerMobile": "033567890", "result_CardEnrolled": "CARD_ENROLLED", "c3DSecureID": "20190330160531033931", "aR_Simple_Html": "<!DOCTYPE HTML PUBLIC "-//W3C// DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/ html4/loose.dtd"><html><head><title>Process Secure Payment</title><meta http-equiv="content-type" content="text/html; charset=UTF-8"><meta name="description" content="Process Secure Payment"><meta name="robots" content="noindex"><style type="text/css">body {font-family:"Trebuchet MS" sans-serif; background-color: #FFFFFF; }#msg {border:5px solid #666; background-color:#fff; margin:20px; padding:25px; max-width:40em; -webkit-border-radius: 10px; -khtml-border-radius: 10px; -moz-border-radius: 10px; border-radius: 10px;} #submitButton { text-align: center ; }#footnote {font-size:0.8em;}</style></head><body onload=" return window.document.echoForm.submit()"> <form name="echoForm" method="POST" action="https://mtf.gateway.mastercard.com/acs/ MastercardACS/ a94a275d-2cf8-4aea-8446-3708137404d7" accept-charset="UTF-8"> <input type="hidden" name="PaReq" value="eAFVUctygkAQvFvIP1Dcwy4gita4lu8QBQ2aSq4UbJREQHkE4zFfk+ /Kl2TWZ3Kgiu5mmp4e6OyjftB0yxM4rasKISWeOwnQRiv2v LTcnRnyh1WrcBynXI+WHC/SDkDm2eZt+JSGOBmzTSNmIGTGc y7Lt8xONsxdFM0lBeIU6m/9uKcgefvepbDDN3QVQrkDCHiqTVg9qx nTS1ngqMnAmlv4ldasq2+OxtZTtfpD4EcNfCTIs7TT2aYdSAXAE W6Yes832YtQsqyVN68w0Hxk0jZvgMRlpBbpnk0mW43T4M2O 7Fvc8exo1pEoe7w2l8fGw4TdOuP7+WbSDiCwi8nDONqk2q61 RS1RY1WroK5MiDF4lIbD5xpZ+vb41ShYpN Tyxsc+6J4CakP5SgDWneflQhcEfL9NYo6+WM71Hcgte/9etO vn2CMepaGp6C0ejCl6PgrCJcSyMDvGPQMgYpScT4i9HC +MzL/LVyu/YtC1WA=="><input type="hidden" name="TermUrl" value="http://localhost/MerchantSimulator /Merchant </pre>
-------------	--

	<pre> /TestView\ "><input type=\ "hidden\ " name=\ "MD\ " value=\ "\ "><noscript><div id=\ "msg\ "><div id=\ "submitButton\ "><input type=\ "submit\ " value=\ "Click here to continue\ " class=\ "button\ "></div></div></noscript> </form></body> </html>\n", "secureHash": "6B5AB8ABE9DD8CEE7E9BD5786B7ECFA96E76A640E4FC142F A3DCF32DBB431950", "responseCode": "435", "responseMessage": "Card holder is enrolled." } </pre>
--	---

12.15 Process ACS- Request JSON

This is a request to interpret the authentication response returned from the card Issuer's Access Control Server (ACS) after the cardholder completes the authentication process. The response indicates the success or otherwise of the authentication.

Version 1.1

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/API/Purchase/ProcessACSResult
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre> { "pp_TxnType": "MPAY", "pp_TxnRefNo": "T20170416122642", "pp_MerchantID": "Test00127801", "pp_Password": "0123456789", "pp_3dSecureID": "159915", "pp_TxnDateTime": "20170425210900", "pp_TxnExpiryDateTime": "20170426210900", "pp_BillReference": "billRef", "pp_Description": "Description of transaction", "paRes": "xxxxx", "pp_SecureHash": "" } </pre>

Version 2.0

Type	Post
-------------	------

Sandbox URL	http://119.160.80.70/payaxisapplicationapi/API/2.0/Purchase/ProcessACSR esult
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre> "pp_IsRegisteredCustomer": "Yes", "pp_CustomerID": "test", "pp_CustomerEmail": "test@test.com", "pp_CustomerMobile": "033567890", "pp_TxnType": "MPAY", "pp_TxnRefNo": "T20190330150615", "pp_MerchantID": "Merc0003", "pp_Password": "0123456789", "pp_3dSecureID": "20190330160531033931", "pp_TxnDateTime": "20190330150613", "pp_TxnExpiryDateTime": "20190330150613", "pp_BillReference": "billRef", "pp_Description": "Description of transaction", "paRes": "eAHNV2uvokoW/Ss3dz6abkBFscM1KSheSqEgD+E bLwHloYCA/Popj92nz+3bd6Yzk0yGxFjsrNp77aq9ahesmdZxDA9x eK/jNYvipvGT+Lcs+uN3as4w9Jye/75m98ClmzXbxXWTVeWa+ kx+nrLEt1c8qw5Tv2zXrB/eOEVb0zN6RpEs8fWVLeJag Wu04xRV0bZ46svAEt9n7u9PHw3mMGTR+nY05GYjLdWqzG7jQ RL0pbZi0MI59X+wxBPBRn4br6cktSJnM/I3ivpC0l9mFEu82 dnr0x0oqjtmNSXxwxfT SxOt47L8LGmmQVLvL+x8XCtyvg5iSXexyzxnd3VL9d4VZZTCjt9/jAD 7BtbWfO4Ztus+DORkf1liiO82dmm9dt7s3ZZ4uulDf2uW5/lRzlZumJG CRYwBICfTrPihdwxONs3CBuH2Zp8ksL/b7NAnlR11qbFGif9xHw3sM STCvF11w5ZUuKwdfzbUORl88fvadtevxBE3/ef+9nnqk6l5woR5lR gKjJkn/gLX/OiiOlPFVrlvdLvA+hn2ej3+ICQHGbVtFv7wF/5tI0CGq1 WhEO/IS9fgqpefnpaaAoisbuiZ/7fMV9Y/srQV68p++868b/1KQ+9Qzw nvbL0Zo14lP83HNcYjBL4qb9TyJ88/7Rwzd/tp/f4/Uwd90G8oifVS D1RG5COvdt7w1N+9zM17wXkiU+UHRj+23B37m/gH53i+zOvFvdJu of0jUXtQl/PtT9NrHyYCHA7Hintcl27CS0mVDmrLjx0JnJhOEKLSU+ Ai2Pg6kd7RMNnJfMMquKkycGkbVZnGxIxJbm+2bcDMHRaXkvm0X SCQrlQZ7T7vZAOF1SkysX0s5kaIT0ku70wlyMzevsoWZweXqQChi6 JGdpyz9T/IE8u40frzl60uQK+q2/Zp8jPq7b7lSrCssYKQrvQp4H4Y UHdt9D3d1sK09Ju1ADuiBwOuhDKKgIXCRAWQKXlI63rQFCsOUSze ZAYgJKRAYUDASYF2Zail5uruF0kwbFR2yFscBOGr9jeYy1SFtWREO 0KH2QRxC9/CJTz1HdNRIz9FHU7KnnjNAXxKvQUZtdFL05TTUELw MCAozBJUHghblPG3mm416t515Lvkv5BG4L14VaaQ4xweHPfKfHz i4ztCYkv2GEEBIVC9rQHOCz7zQgerV3oX2roOhWGwwhLjJPuCyCGP CrvRp2nqO/PWEShkTfMyKOWHUqQTAqTEH27SQQlUmUBc4oFsAzCUN QJ7LdLz0OrQfzAZaxq4LrFsM7UxXTToCT58vhzjCHXit08mo+nWkZ w10z8qQKu1y5qkRNbuRG7i8XHlvspEtXxv11t+t5p8Lkp49berg5nc O7dxDzDTrz2/ODWVWTveGRB/6uibTvcKslztnnW987mndnvxiKU V5Nk4U8nU+p+wrpAjW5H5sEnFurt4JaVyDQAfdjThx4y4kDoKBER 1zRQRKcdFm/6jtXk0+H8pG7i50x03b0qdy6voLbAlPlaJWGgdU2 </pre>

	e/WuLhwi2wU0h8tv7nkiXOn3ZdzPw2jltJP5JQnFk5LcR14ryxpN 4CIU2OL9PlIkQfcZCkW1AlIvarGqv3ge8LZy5uKEXx66ZwA3++u G+2h3xdbsjlX2WWWWeBVL/Kign0rKPGNJBSGPJfRTSQXj/1BSZx C+S8r+W0LB3QSx2JP9zhR6ZIY9GsGIRtHHtuFls95tSAYDP4LNy69 rgotol73v+eSt1BWh1wxT0AfBBPsXJjR5YfPwj1rmOnT+AbvFWMv M0QdsY/KiJhoPzjJszUIG08v6Nwl5fyuhg6VxvyYdvguTZhlcAmpy4 XZVPqaOqlfn221K04lAoivZ8+JQtLebtHOosV5lMogW/TLbMemBVG znqZtm+ZgYHa3pNK/VHK0loxdRj0nkC2ejELx0oZ/obqlmhZqc SsRwNhwlggt0xqUsj+be5bwsHY6KPDke9e2D4iJePoy7br61N5SG vKVu+Gd4tft/lx1xd+7cjlJnrxZYDU1/kFf5o17KcRLeUXHMmeLBP zyQt66XZryWjdnAe7ysisEquQRuTV7ruzK2VHq4HMMz4W6iOqVqF yx5L9f2pSSqxJk8Ma5M1wkjgwc02uNwyftt683gMA48k9nal9eZeSQd aO9+aE0+PGS+m+wuWe1I9i1tFZ5kOCH7NelAZGLpXG8J6BXCxJQN2 ExqnrRBkdLXv5wg+FREEvM/LMV5L4NvpWj/bSn+tTuhp3ToP3enr7 Yz1yG96fIXiUtCv+Fs80Mn4XAnsQYBGfgoeXUSWehTPizy0S3Eu/cRm yJoC7T5AatirGLYYWILtmlDIUZc/9ahwlBsW95Q4czlPYhL7ujlgaBvr pPf1V+WEtQUEpmniOIEmjvbpuu2Xq5ORMozy+QaJtQ+liunTkJqc aEunma6F/4aTxLxtNxuHFrtZx2QBMsrxWaale6tpShm+TL3Z/f0 27SVCD21MBWfNcK9j1/u4H2SHukDot0Oa6Ole4v3TxMztXsBJgy 5m6eVsEorVPBK+gkSiblyAKQW+pgzb5KqZrLFLJkA3HkcX0imOgO xxk1M70JanS4blV1yTiTRm+6+aUeOxt33Oq5NwZ55hTJw0eMk/ wr/FYcr3iH/i+PePdHPb3VQiTOuogA4sCJ+bFdifgGCBNXAEK45ww6 DufxFAPvd5nmnFReVuKCL253O4XFLShFGRZdflwKhZ0w4362CsZlK vUO5CdyoVpDol5OslTWSTRP3NltNTUJBxyZzXSIYqAvzVPWqZW2 4JekzZBJpAU6vjGLVhRG5VQT7NaepPC0t2G1WzlcXsz2cb5CpuTJ 1yG6Lc/5SmlFLyLxVfgvXfrN8roDE+/34u83ZvzZ8vULHI/+9GX+ T7APIF8=", "pp_SecureHash": "1B7082A29290BF22219A5F2C27BAEAB4F5 E35E0B788343B4C0CEF052D08F7E16" }
--	---

12.16 Process ACS - Response JSON

Version 1.1

Body	<pre>{ "c3dSecureID": "", "gatewayCode": "", "responseCode": "", "responseMessage": "" }</pre>
-------------	--

Version 2.0

Body	<pre>{ "c3DSecureID": "20190330160531033931", "summaryStatus": "AUTHENTICATION_SUCCESSFUL", "gateWayCode": "AUTHENTICATION_SUCCESSFUL", "secureHash": "958BE413012C18561FA67FCFCE5F7DF6050BE3EB97377CC FDB1017B51FF90E14", "responseCode": "445", "responseMessage": "The cardholder was successfully authenticated by the card Issuer." }</pre>
-------------	--

12.17 Payment Direct Pay -Request JSON

This is a single transaction to authorise the payment and transfer funds from the payer's account to your Merchant's account.

Version 1.1

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/API/Purchase/PAY
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre>{ "pp_Version": "1.1", "pp_TxnType": "MPAY", "pp_TxnRefNo": "T20170518161116", "pp_MerchantID": "Test00127801", "pp_Password": "0123456789", "pp_Amount": "10000", "pp_TxnCurrency": "PKR", "pp_TxnDateTime": "20170518161116", "pp_TxnExpiryDateTime": "20170520161116", "pp_BillReference": "billRef", "pp_Description": "Description of transaction", "pp_CustomerCardNumber": "5123450000000008", "pp_CustomerCardExpiry": "0517", "pp_CustomerCardCvv": "100", "pp_SecureHash": "", "pp_Frequency": "RECURRING" }</pre>

--	--

Version 2.0

Type	Post
Sandbox URL	http://119.160.80.70/payaxisapplicationapi/API/2.0/Purchase/PAY
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre> { "pp_IsRegisteredCustomer": "Yes", "pp_ShouldTokenizeCardNumber" : "Yes", "pp_CustomerID": "test", "pp_CustomerEmail": "test@test.com", "pp_CustomerMobile": "0336789043", "pp_TxnType": "MPAY", "pp_TxnRefNo": "T20190329131312", "pp_MerchantID": "Merc0003", "pp_Password": "0123456789", "pp_Amount": "20000", "pp_TxnCurrency": "PKR", "pp_TxnDateTime": "20190329131312", "pp_C3DSecureID": "20190328100447620695", "pp_TxnExpiryDateTime": "20190329131310", "pp_BillReference": "billRef", "pp_Description": "Description of transaction", "pp_CustomerCardNumber": "5457210001000019", "pp_CustomerCardExpiry": "1120", "pp_CustomerCardCvv": "123", "pp_SecureHash": "1B7082A29290BF22219A5F2C27BAEAB4F5E35E0B788343 B4C0CEF052D08F7E16" } </pre>

12.18 Payment Direct

Pay -Response

JSON

Version 1.1

Body	<pre>{ "responseCode": "", "responseMessage": "" }</pre>
-------------	--

Version 2.0

Body	<pre>{ "pp_TxnType": "MPAY", "pp_MerchantID": "MERC0003", "pp_Language": "EN", "pp_SubMerchantID": "", "pp_BankID": "", "pp_ProductID": "", "pp_TxnRefNo": "T20190401095125", "pp_Amount": "20000", "pp_TxnCurrency": "PKR", "pp_TxnDateTime": "20190401095125", "pp_TxnExpiryDateTime": "", "pp_BillReference": "billRef", "pp_Description": "Description of transaction", "pp_ReturnURL": "", "ppmpf_1": "", "ppmpf_2": "", "ppmpf_3": "", "ppmpf_4": "", "ppmpf_5": "", "ppmpf_6": "", "ppmbf_1": "", "ppmbf_2": "", "ppmbf_3": "", "ppmbf_4": "", "ppmbf_5": "", "ppmbf_6": "", "pp_Frequency": "SINGLE", "pp_RetreivalReferenceNo": "190401301391", "pp_TokenizationResponseCode": "T01", }</pre>
-------------	--

	<pre> "pp_TokenizationResponseMsg": "The card tokenizati on request has been accepted.You will be shortly notified on your system about its status", "pp_CustomerID": "test1", "pp_CustomerEmail": "test2@test.com", "pp_CustomerMobile": "0346789567", "pp_C3DSecureID": "", "pp_ShouldTokenizeCardNumber": "No", "pp_IsRegisteredCustomer": "Yes", "pp_SecureHash": "12DDF069C1C6B0FC5AAE838A010285DAEC8D45843E2B4 6CFC983AE320C04C714", "pp_InstrToken": null, "responseCode": "000", "responseMessage": "Thank you, your transaction was successful. " } </pre>
--	--

13. Tokenization API

13.1 Delete Token API

This request will delete the saved token against the provided field of TokenizedCardNumber.

Type	Post
Example URL	http://localhost/PayAxisAPI/api/v1.0/tokenization/deletetoken
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre> { "pp_Language": "EN", "pp_CorrelationId": "Merc0003DEL00013", "pp_IsRegisteredCustomer": "Yes", "pp_MerchantID": "Merc0003", "pp_Password": "0123456789", "pp_InstrumentType": "CARD", "pp_TokenizedCardNumber": "9053845788156268", "pp_SecureHash": "94108C9664C1CB49F1D63A671F178D9EC60944FDEC4FFE7D277535BFDDC00673" } </pre>

Response	<pre>{ "pp_Language": "EN", "pp_MerchantID": "Merc0003", "pp_SecureHash": "61CC64C0FC41848E31D1A1B00FA21BD32BBF2610C68307B629DEAF3D9F3B8518", "pp_Password": "0123456789", "pp_InstrumentType": "CARD", "pp_TokenizedCardNumber": "9774917123133985", "pp_CorrelationId": "Merc0003DEL00043", "pp_IsRegisteredCustomer": "yes", "pp_ResponseCode": "T00", "pp_ResponseMessage": "The tokenization operation was successfully processed" }</pre>
-----------------	---

13.2 Instant Token Notification (ITN)

Merchant will be required to expose a Rest based API for Payment Gateway to notify about the Tokenized card status whenever any crucial operation occurred at the gateway like (CREATE or UPDATE or DELETE) token.

So that Merchant can take action in its system on the basis of **ApiOperation** field received in ITN call.

Version 1.0

Type	Post
Example URL	http://www.sampleurl.com/api/2.0/UpdateToken
Production URL	Will be communicated after business approval
Headers	application/json

Body	<pre>{ "pp_Version": "1.0", "pp_CustomerID": "10000987", "pp_TxnRefNo": "T20190327181830", "pp_MerchantID": "Merc0003", "pp_TokenizationResponseCode": "T00", "pp_TokenizationResponseMsg": "The tokenization operation was successfully processed", "pp_CustomerCardNo": "512345*****2346", "pp_CustomerCardExpiry": "0521", "pp_TokenizedCardNumber": "9053845788156268", "pp_LastModificationDateTime": "20190327181830", "pp_CorrelationId": null, "pp_ApiOperation": "CREATE", "pp_SecureHash": "413FCCAB4BEDBB352109E679EA2779825183058232DB9A864B3CB707EBD06374" }</pre>
Response	<pre>{ "pp_ResponseCode": "000", "pp_ResponseMessage": "Success" "pp_SecureHash" 063E4AADE24337CF501D95FB4C5CBDC65F78D8217B11564371CE22AD6B4129B9" }</pre>

13.3 Check3DSEnvironmentViaToken

This request will delete the saved token against the provided field of TokenizedCardNumber.

Version 2.0

Type	Post
-------------	------



Response

	<pre> r:#fff; margin:20px; padding:25px; max- width:40em ; -webkit-border-radius: 10px; -khtml-border- radius: 1 0px; -moz-border-radius: 10px; border-radius: 10px;} #submitButton { text-align: center ; }#footnote {font- size:0.8em;}</style></head><body onload=\"return window.document.echoForm.submit()\"><form name=\"echoForm\" method=\"POST\" action=\"https://mtf.gateway.mastercard.com/ac s/ MastercardACS/cd4d9396-fe10-4182-a62d- 2da086d5d666\" accept-charset=\"UTF-8\"><input type=\"hidden\" name=\"PaReq\" value=\"eAFVUctuwjAQvCPxD1HujZ2E0IAWI15V U8pDkLbqqbKMBZESBww06bVf0+/ql3QdoLQ3z4x3d 3YWum WWWu9S75N cdWzXobYllchXiVp37Kf47ia0u6xeg3ijpRwupThqyW Ai93u+llaywpq AUt9vBjaDeW8hdwzO7Rh2czwgF4hVWmy40jDgYte PpizwA9+lQ M4QMqmjIZvM+o/RdPwWz8ZAThQonkkjREaxUBlNr Xi0jIFUCoj8 qA76gwVhE8gFwFGnrCgKR5Y826bSEXkGxJBAr17mR +Nqj1uVyYr 1XtZip3oPdDQrZ+k2fB0Ug2c/X0ZcdICYH7DiB8k86r Zog3qWG7 Y92qY4tuKBZ8YKm48X1vfnl0epQ82GJxa2ZljvBFAz0 l8KMF6N +V8WuSCQ5TZXEvtinr9vIFfvg3uTqjhgf0Hr+Y2geRu2 qHmhs7 NguiQYEjoPqzYGADGL5Hw6zKW6LDL/Ll6v/QAxQLM 6\"> <input type=\"hidden\" name=\"TermUrl\" value=\"http://localhost/MerchantSimulator /Merchant /TestView\"><input type=\"hidden\" name=\"MD\" value=\"\"><noscript> <div id=\"msg\"><div id=\"submitButton\"><input type=\"submit\" value= \"Click here to continue\" class=\"button\"></div></div></noscript> </form></body></html>\n", "secureHash": "79FC7837113546D70D3A03FCA509DFF982DA695D161 A7D5CE43372C129D0B122", </pre>
--	--

	<pre> "pp_IsRegisteredCustomer": "Yes", "pp_TokenizedCardNumber": "9790662127634170", "responseCode": "435", "responseMessage": "Card holder is enrolled." } </pre>
--	---

13.4 ProcessACSViaToken

This request will delete the saved token against the provided field of TokenizedCardNumber.

Version 2.0

Type	Post
Example URL	http://localhost/PayAxisAPI/api/2.0/purchase/ProcessACSResultViaToken
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre> { "pp_IsRegisteredCustomer": "Yes", "pp_CustomerID": "test", "pp_CustomerEmail": "test@test.com", "pp_CustomerMobile": "033567890", "pp_TxnType": "MPAY", "pp_TxnRefNo": "T20190330150615", "pp_MerchantID": "Merc0003", "pp_Password": "0123456789", "pp_3dSecureID": "20190330160531033931", "pp_TxnDateTime": "20190330150613", "pp_TxnExpiryDateTime": "20190330150613", "pp_BillReference": "billRef", "pp_Description": "Description of transaction", "paRes": "eAHNV2uvokoW/Ss3dz6abkBFscM1KSheS qEgD+EbLwHloYCA/Popj92nz+3bd6Yzk0yGxFjsrN p77aq9ahesmdZxDA9xeK/jNYvipvGT+Lcs+uN3as4 w9Jye/75m98CImzXbxXWTVeWa+kx+nrLEt1c8qw 5Tv2zXrB/eOEVB0zN6RpEs8fWVLeJagWu04xRV0b </pre>

		Z46svAEt9n7u9PHw3mMGTR+nY05GYjLdWqzG7j QRL0pbZi0MI59X+wxBPBRn4br6cktSJnM/I3ivpC0l 9mFEu82dnr0x0oqjtmNSXxwXlFTSxOt47L8LGmm QVLvL+x8XCtyvg5iSXexyzxnd3VL9d4VZZTCjt9/jA D7BtbWfO4Ztus+DOrKf1liiO82dmm9dt7s3ZZ4uul Df2uW5/IRzlZumJGCRYwBICfTrPihdwxONS3CBuH 2Zp8ksL/b7NAnIR11qbFGif9xHw3sMSTCvF11w5Z UuKwdfzbUORl88fvadtevxBE3/ef+9nnqk6l5woR5l rAgKjJkn/gLX/OiiOlPFVrlvdLvA+hn2ej3+ICQHGbV tFv7wF/5tI0CGq1WhEO/IS9fgqpefnpaaAoisbuiZ/ 7fMV9Y/srQV68p++868b/1KQ+9QzwnvbL0Zo14lP 83HNcYjBL4qb9TyJ88/7Rwzd/tp/f4/Uwd90G8oif VSD1RG5COvdt7w1N+9zM17wXkiU+UHRj+23B37m /gH53i+zOvFvdJuof0jUXtQL/PtT9NrHyYCHA7Hint cl27CS0mVDmrLjx0JnJhOEKLSU+Ai2Pg6kd7RMNn JfMMqukKycGkbVZnGxIxJbm+2bcDMHRaXkvm0XS CQrlQZ7T7vZAOF1SkysX0s5kalT0ku70wlyMZevso WZweXqQCHi6JGdpyz9T/IE8u40frzl60uQK+q2/Z p8jPq7b7ISrCsYKQrvQp4H4YUHDt9D3d1sK09Ju1 ADuiBwOuhDKKgIXCRAWQKXIl63rQFCsOUSzeZAYg JKRAYUDASYF2ZAil5uruF0kwbFR2yFscbOGr9jeYy 1SFtWREO0KH2QRxC9/CJTz11HdNRiz9FHU7Knnj NAXxKvQUZtdFL05TTUELwMCAozBJUHghblPG3m m416t515Lvkv5BG4L14VaaQ4xweHPfkFhZi4ztCY kv2GEEBIVC9rQHOCz7zQgerV3oX2roOhWGwwhLj JPuCyCGPCrvRp2nqO/PWEShktfMyKOWHUqQTAq TEH27SQQlmUBc4oFsAzCUNQJ7LdLz00rQfzAZax q4LrFsm7UxXTToCT58vhzjCHXitO8mo+nWkZw10z8 qQKu1y5qkRNbuRG7i8XHlvspEtXxv11t+t5p8Lkp49 berg5ncO7dxDzDTrz2/ODWVWTveGRB/6uibTVcK SlztnnW987mndnvxiKUV5Nk4U8nU+p+wrpAjW5H 5sEnFurt4JaVyDQAfdjThx4y4kDoKBER1zRQRKcdF m/6jtXk0+H8pG7i50xO3b0qdy6voLbAlPlaJWGgd U2e/WuLhwi2wU0h8tv7nkiXOn3ZdzPw2jltJP5JQ nFk5LcR14ryxpN4CIU2OL9PlIkQfcZCkW1AllvarG qv3ge8LZy5uKEXx66ZwA3++uG+2h3xdbsjIX2WW WeBVL/Kign0rKPGNJBSGPJfRTSQXj/1BSZxC+S8r+ W0lB3QSx2JP9zhR6ZIY9GsGIRtHHtuFls95tSAYDP4 LNy69rgotol73v+eSt1BWh1wxT0AfBBPsXJjR5YfP wj1rmOnT+AbvFWMvM0QdsY/KiJhoPzjJszUIG08v 6Nwl5fyuhg6VxvyYdvguTZhlcAmpy4XZVPqaQqlfn 221K04lAoivZ8+JQtLebtHOosV5lMogW/TLbMemB VGzNqZtm+ZgYHa3pNK/VHK0loxdRj0nkC2ejELx0 oZ/obqlmhZqcSsRwNhwlggt0xqUsj+be5bwsHY6K PDke9e2D4iJePoy7br61N5SGvKVu+Gd4tft/lx1xd+ 7cjlJnxrZYDU1/kFf5o17KcRLeUXHMmeLBPzyQt66 XZryWjdnAe7ysisEquQRuTV7ruzK2VHq4HMMz4W 6iOqVqFyx5L9f2pSSqxJk8Ma5M1wkjgwc02uNwyft
--	--	---

	<pre>t683gMA48k9naI9eZeSQdaO9+aE0+PGS+m+wuWe 1I9i1tFZ5kOCH7NeIAZGLpXG8J6BXcXJQN2ExqnrR BkdLXv5wg+FREEvM/LMV5L4NvpWj/bSn+tTuhp3 ToP3enr7Yz1yG96fLXiUtCv+Fs80Mn4XAnsQYBGfgo eXUSWehTPizy0S3Eu/cRmyJoC7T5AatirGLYYWILt mlDIUZc/9ahwlBsW95Q4czlPYhL7ujlgaBVrpPf1V+ WEtQUEpmniOLEMjvbpuu2Xq5ORMozy+QaJtQ+liu nTkJqcaEunma6F/4aTxLxtNxuHFrtZx2QBMsrxaW aale6tpShm+Tl3Z/f027SVCD21MBWfNck9j1/u4H2 SHukDot0Oa6Ole4v3TxMztXsBJgy5m6eVsEorVPBK +gkSiblYaKQW+pgzb5KqZrLFLJkA3Hkcx0imOgOxx k1M70JanS4bLV1yTiTRm+6+aUeOxt33Oq5NwZ55h TJw0eMk/wr/FYcr3iH/i+PePdHPb3VQiT0uogA4s CJ+bFdifgGCBNXAEK45ww6DufxFAPvd5nmnFReV uKCL253O4XFLShFGRZdflwKhZ0w4362CsZlKvUO5 CdyoVpDol5OslTWSTRP3NltNTUJBxyZzXSIYqAvzV PWqZW24JekzZBJpAU6vjGLVhRG5VQT7NaepPC0 t2G1WzlcxSz2cb5CpuTJ1yG6Lc/5SmlFLyLxVfgvXf rN8roDE+/34u83ZvzZ8vULHI/+9GX+T7APIF8=", "pp_SecureHash": "1B7082A29290BF22219A5F2C27BAEAB4F5E35E0B 788343B4C0CEF052D08F7E16"</pre>
Response	<pre>{ "c3DSecureID": "20190330160531033931", "summaryStatus": "AUTHENTICATION_SUCCESSFUL", "gateWayCode": "AUTHENTICATION_SUCCESSFUL", "secureHash": "958BE413012C18561FA67FCFCE5F7DF6050BE3EB 97377CCFDB1017B51FF90E14", "responseCode": "445", "responseMessage": "The cardholder was successfully authenticated by the card Issuer." }</pre>

13.5 PayViaToken

Version 2.0

Type	Post
Example URL	http://localhost/PayAxisAPI/api/2.0/purchase/PayViaToken
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre>{ "pp_IsRegisteredCustomer": "Yes", "pp_CustomerID": "testPay", "pp_CustomerEmail": "test@test.com", "pp_CustomerMobile": "033456789025", "pp_TxnType": "MPAY", "pp_C3DSecureID": "", "pp_TxnRefNo": "T20190403093759", "pp_MerchantID": "Merc0003", "pp_Password": "0123456789", "pp_Amount": "20000", "pp_TxnCurrency": "PKR", "pp_TxnDateTime": "20190403093750", "pp_TxnExpiryDateTime": "20190403093747", "pp_BillReference": "billRef", "pp_Description": "Description of pay transaction", "pp_TokenizedCardNumber": "9790662127634170", "pp_CustomerCardCvv": "123", "pp_SecureHash": "1B7082A29290BF22219A5F2C27BAEAB4F5E35E0B788343B4C0CEF052D08F7E16" }</pre>
<u>Response</u>	<pre>{ "pp_TxnType": "MPAY", "pp_MerchantID": "MERC0003", "pp_Language": "EN", "pp_SubMerchantID": "", "pp_BankID": "", "pp_ProductID": "", "pp_TxnRefNo": "T20190403093759", "pp_Amount": "20000", "pp_TxnCurrency": "PKR", "pp_TxnDateTime": "20190403093750", "pp_TxnExpiryDateTime": "", "pp_BillReference": "billRef", "pp_Description": "Description of pay transaction", "pp_ReturnURL": "", "ppmpf_1": "" }</pre>

	<pre> "ppmpf_2": "", "ppmpf_3": "", "ppmpf_4": "", "ppmpf_5": "", "ppmpf_6": "", "ppmbf_1": "", "ppmbf_2": "", "ppmbf_3": "", "ppmbf_4": "", "ppmbf_5": "", "ppmbf_6": "", "pp_RetreivalReferenceNo": "190403301554", "pp_CustomerID": "testPay", "pp_CustomerEmail": "test@test.com", "pp_CustomerMobile": "033456789025", "pp_CustomerCardNo": "512345*****2346", "pp_CustomerCardExpiry": "0819", "pp_SecureHash": "61B9869E834E90401B6D0A3278FAA0464597250A4 F8880DAE4FC3055D78D1168", "pp_IsRegisteredCustomer": "Yes", "pp_TokenizedCardNumber": "9790662127634170", "pp_C3DSecureID": "", "responseCode": "000", "responseMessage": "Thank you for Using JazzCash, your transaction was successful. " </pre>
	}

13.6 Retrieve Token

This request will retrieve the saved token against the provided field of TokenizedCardNumber.

Type	Post
Example URL	localhost/PayAxisAPI/api/v1.0/tokenization/retrievetoken
Production URL	Will be communicated after business approval
Headers	application/json
Body	<pre>{ "pp_Language": "EN", "pp_CorrelationId": "Transaction10200109010", "pp_IsRegisteredCustomer": "Yes", "pp_MerchantID": "Merc0003", "pp_Password": "0123456789", "pp_InstrumentType": "CARD", "pp_TokenizedCardNumber": "9292352958920640", "pp_TransactionType": "MPAY", "pp_SecureHash": "10D859C9FFBA5AA04635A700F343CF1271589B831D88607D14155444829B073D" }</pre>
Response	<pre>{ "pp_Brand": "MASTERCARD", "pp_Expiry": "1120", "pp_FundingMethod": "DEBIT", "pp_Issuer": "CAPITAL ONE BANK (CANADA BRANCH)", "pp_LocalBrand": "MASTERCARD", "pp_cardNumber": "545721xxxxxx0019", "pp_tokenStatus": "VALID", "pp_Language": "EN", "pp_MerchantID": "Merc0003", "pp_SecureHash": "81B9A589239D9563E1CBEC82FA3BCE62B718935DECD58BBC435EE85521F4582A", "pp_Password": "0123456789", "pp_InstrumentType": "CARD", "pp_TokenizedCardNumber": "9292352958920640", "pp_CorrelationId": "Transaction10200109010", "pp_IsRegisteredCustomer": "Yes", "pp_ResponseCode": "T00", }</pre>

	<pre>"pp_ResponseMessage": "The tokenization operation was successfully processed" }</pre>
--	--

14. Calculating and Validating the Secure Hash

Secure Hash is used to detect whether a transaction request and response has been tampered with. The Shared Secret generated for merchant at the time of its registration is added to the transaction message and then an SHA256 algorithm is applied to generate a secure hash. The secure hash is then sent to the receiving entity with the transaction message. Because the receiving entity is the only other entity apart from transaction initiator that knows the shared secret it recreates the same secure hash and matches it with the one in the request message. If the secure hash matches, the receiving entity continues processing the transaction. If it doesn't match, it assumes that the transaction request has been tampered with and will stop processing the transaction and send back an error message. This is a security feature to secure the transaction and is recommended but its not mandatory.

14.1 How the Secure Hash is Created and Verified

The pp_SecureHash field is used for the SHA256 secure hash of initiator's shared secret and the transaction request. The secure hash value is the Hex encoded SHA256 output of the transaction request or response fields. The order that the fields are hashed in are:

1. The Shared Secret (shared between the PG and a merchant), the system generated value, is always first.
2. Then all transaction request fields are concatenated to the Shared Secret in alphabetical order of the field name. The sort should be in ascending order of the ASCII value of each field string. If one string is an exact substring of another, the smaller string should be before the longer string. For example, Card should come before CardNum.
3. Fields must not have any separators between them and must not include any null terminating characters. For example, if the Shared Secret is **0F5DD14AE2E38C7EBD8814D29CF6F6F0**, and the transaction request includes the following fields:

Parameter	Sample Values
pp_MerchantID	MER123
pp_OrderInfo	A48cvE28
pp_Amount	2995

Example of a Secure Hash Calculation

In ascending alphabetical order the transaction request fields inputted to the **SHA256** hash would be:

0F5DD14AE2E38C7EBD8814D29CF6F6F02995MER123A48cvE28

Merchant should also ensure that:

1. UTF-8 encoding should be used to convert the input from a printable string to a byte array. Note that 7-bit ASCII encoding is unchanged for UTF-8.
2. The hash output must be hex-encoded.

14.2 How is SHA256-HMAC Calculated

The SHA-256 HMAC is calculated as follows:

1. The SHA-256 HMAC calculation includes all PP fields, that is, all fields beginning with "PP"
2. All transaction fields are concatenated in alphabetical order of the ASCII value of each field string with '&' after every field except the last field.
3. To this concatenated string, Shared Secret is prepended.
4. This string is first converted into UTF8 bytes and then it is converted into ISO-8859-1 encoding.
5. The ISO-8859-1 string is then hashed using HMAC with UTF-8 encoded Shared Secret as key.
6. The generated hash is then converted into hexadecimal

Example of a Secure Hash Calculation

Parameter	Sample Values
pp_MerchantID	MER123
pp_OrderInfo	A48cvE28
pp_Amount	2995

In ascending alphabetical order the transaction request fields inputted to the **SHA256-HMAC** hash would be:

0F5DD14AE2&2995&MER123&A48cvE28

Merchant should also ensure that:

7. UTF-8 encoding should be used to convert the input from a printable string to a byte array. Note that 7-bit ASCII encoding is unchanged for UTF-8.

The hash output must be hex-encoded.

15. Padding Rules

Following are the padding rules that should be followed for all the messages described in this document:

Message Format	Data Type	Formatting
Fixed Length	AN	Postfix with spaces to reach the prescribed length
Fixed Length	N	Prefix with 0
Web service invoke	AN	Not required
Web service invoke	N	Not required

16. Appendix I - Response Code

Payment Response Code

Payment Response Code	Response Code Description
000	Thank you for Using JazzCash, your transaction was successful.
001	Limit exceeded
002	Account not found
003	Account inactive
004	Low balance
014	Warm card
015	Hot card
016	Invalid card status
024	Bad PIN
055	Host link down
058	Transaction timed out
059	Transaction rejected by host
060	PIN retries exhausted
062	Host offline
063	Destination not found
066	No transactions allowed
067	Invalid account status
095	Transaction rejected
101	Invalid merchant credentials
102	Card blocked
103	Customer blocked
104	BIN not allowed for use on merchant
105	Transaction exceeds merchant per transaction limit

106	Transaction exceeds per transaction limit for card
107	Transaction exceeds cycle limit for card
108	Authorization of customer registration required
109	Transaction does not exist.
110	Invalid value for <field name>
111	Transaction not allowed on Merchant/Bank
112	Transaction Cancelled by User
113	Transaction settlement period lapsed
115	Invalid hash received
116	Transaction Expired
117	Transaction not allowed on Sub Merchant
118	Transaction not allowed due to maintenance
119	Transaction is awaiting Reversal
120	Delivery status cannot be updated
121	Transaction has been marked confirmed by Merchant
122	Reversed
124	Order is placed and waiting for financials to be received over the counter.
125	Order has been delivered
126	Transaction is disputed
127	Sorry! Transaction is not allowed due to maintenance.
128	Awaiting action by scheme on Dispute
129	Transaction is dropped.
131	Transaction is Refunded.
132	Sorry! The selected transaction cannot be refunded.
134	Transaction has been timed out.
135	Invalid BIN was entered for discount.
157	Transaction is pending.(for Mwallet and Mlgs)
199	System error
200	Transaction approved - Post authorization
210	Authorization pending
401	Sorry! Your transaction could not be processed at this time, please try again after few minutes.
402	Your transaction was declined by your bank, please contact your bank
403	Your transaction has timed out, please try again
404	Your transaction was declined because your card is expired, please use a valid card
405	Your transaction was declined because of insufficient balance in your card
406	Sorry! Your transaction could not be processed at this time due to system error, please try again after few minutes
407	Sorry! Your transaction could not be processed at this time due to internal system error, please try again after few minutes
408	Your bank does not support internet transactions, please contact your bank
409	Transaction declined - do not contact issuer
410	You have aborted the transaction, Our team will contact you shortly to assist you or you can share your feedback with us via emailing us at :

411	Sorry! Your transaction is blocked due to risk, please use any other card and try again
412	You have aborted the transaction, Our team will contact you shortly to assist you or you can share your feedback with us via emailing us at :
414	Sorry! Your transaction was declined, please contact your bank
415	Your 3D Secure ID verification was failed, please use correct ID and try again.
416	Your CVV verification was failed, please use correct CVV and try again, click the help button “?” In CVV tab to find out the details of CVV.
417	Order locked - another transaction is in progress for this order
419	Your Card is not enrolled in 3D secure, please contact your bank and active your 3D secure ID
421	Your retry limit is exhausted, please contact your bank
422	Your transaction was declined due to duplication, please try again
423	Your transaction was declined due to address verification failed, please try again
424	Your transaction was declined due to wrong CVV, please try again with correct CVV, click the help button “?” In CVV tab to find out the details of CVV
425	Transaction declined due to address verification and card security code
426	Transaction declined due to payment plan, please contact your issuer bank
429	Your transaction has not been processed this time, please try again or contact your issuer bank.
430	Request_rejected
431	Server_failed
432	Server_busy
433	Not_enrolled_no_error_details
434	Not_enrolled_error_details_provided
435	Card_enrolled
436	Enrollment_status_undetermined_no_error_details
437	Enrollment_status_undetermined_error_details_provided
438	Invalid_directory_server_credentials
439	Error_parsing_check_enrollment_response
440	Error_communicating_with_directory_server
441	Mpi_processing_error
442	Error_parsing_authentication_response
443	Invalid_signature_on_authentication_response
444	Acs_session_timeout
446	Authentication_failed
448	Card_does_not_support_3ds
449	Authentication_not_available_no_error_details
450	Authentication_not_available_error_details_provided
999	Transaction failed. This response code will be sent when the transaction fails due to some technical issue at PG or Bank’s end.

Tokenization Response Code

Tokenization Response Code	Response Code Description
T00	The tokenization operation was successfully processed
T99	The tokenization operation was declined or rejected by the gateway, acquirer or issuer
T98	The tokenization operation resulted in an internal error and hence cannot be processed
T97	The tokenization operation resulted in an external error and hence cannot be processed
T89	The tokenization operation resulted in an internal error, while inserting token and hence cannot be processed
T88	Request validation failed
110	Validation Errors at the time of tokenization with complete error details
T49	Tokenized Card Number Provided is Invalid
T59	The delete token operation resulted in an internal error and hence cannot be processed
T48	Tokenized Card Number Provided is Expired.
T89	The create token operation resulted in an internal error and hence cannot be processed
144	The customer has selected to discontinue the transaction.
198	Transaction cannot be processed because customer has selected to delete the Expired card.

17. Appendix II- Amount Values for Generating Different Response in Test Environment

As described earlier, when merchant is connected with the test system for performing integration testing the merchant will need to provide different amounts to the Payment Portal for generating different responses in the test environment. Below is the list of the amount that will be provided as input and corresponding output response code. For successful transaction response, an amount of PKR 10000 will be provided as transaction amount.

Response Code	Amount (AED)	Response Code Description
000	10000	Transaction processed successfully.
001	10100	Limit exceeded
002	10200	Account not found
003	10300	Account inactive
004	10400	Low balance
014	10500	Warm card
015	10600	Hot card
016	10700	Invalid card status
024	10800	Bad PIN
055	10900	Host link down
058	11000	Transaction timed out
059	11100	Transaction rejected by host

060	11200	PIN retries exhausted
062	11300	Host offline
063	11400	Destination not found
066	11500	No transactions allowed
067	11600	Invalid account status
095	11700	Transaction rejected
101	11800	Invalid merchant credentials
102	11900	Card blocked
103	12000	Customer blocked
104	12100	BIN not allowed for use on merchant
105	12200	Transaction exceeds merchant per transaction limit
106	12300	Transaction exceeds per transaction limit for card
107	12400	Transaction exceeds cycle limit for card
108	12500	Authorization of customer registration required
109	12600	Transaction does not exist.
110	12700	Invalid value for <field name>
111	12800	Transaction not allowed on Merchant/Bank
112	12900	Transaction Cancelled by User
113	13000	Bank Credentials not generated
115	13200	Invalid hash received
116	13300	Transaction Expired
117	13400	Transaction not allowed on Sub Merchant
118	13500	Transaction not allowed due to maintenance
119	13600	Transaction is awaiting Reversal
120	13700	Delivery status cannot be updated
121	13800	Transaction has been marked confirmed by Merchant
122	13900	Reversed
199	14000	System error
200	14100	Transaction approved - Post authorization (for direct debit)
210	14200	Authorization pending (for direct debit)
999	14300	Transaction failed

18. Appendix III - Fixed Length

In response to a service call, the output returned will always be a fixed length string, the details of which are mentioned below.

In case if any numeric value is less than the required length or empty it will be left padded with zeros.

In case if any alpha numeric field is less than the required length or empty it will be right padded with spaces.