http://jobs.mobilinkgsm.com/i/mobilink-v2/logo.png

****

**INTEGRATION GUIDE FOR MERCHANTS**

***Version 3.7***

***24 March 2017***

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This is unpublished, confidential document of TPS Pakistan Pvt Ltd.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

Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Status | Change Reference |
| 15th 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. |
| 22nd April 2014 | Usman Danish | Format, Appendix III fixed length | Updated section: 14 |
| 29th April 2014 | Mohammad Furqan Zakeria | Made Bank ID field as Mandatory in Payment Status Update | section 8.1 |
| 30th April 2014 | Bina Khan | Removed Customer IBAN fields and updated length of Bank ID field. | Sections 6.2 and 8.1. |
| 7th 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 |
| 25th December 2015 | Adeel Siddiqui | Revision of document | Complete document |
| 16th June 2016 | Adeel Siddiqui | Revision of Payment Status Update | Sections 8, 8.1, 8.2, 8.3 |
| 26th July 2016 | Iqbal Maskati | Addition of HMAC calculation | Sub section 11.2 |
| 16th 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 |
| 25th August, 2016 | Zia Ur Rehman | OTC Payment API Module | Section 11 |
| 09th Sept, 2016 | Iqbal Maskati | Status Update in All transaction types. Added response Codes | Section 8,14 |
| 6th January, 2016 | Muhammad Mujtaba | ASCII:32 will be used for white space in inquiry response | Section 7.2 |
| 24th March | 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 |

Table of Contents

[1 Overview 7](#_Toc478379024)

[1.1 Who Should Read This Guide 7](#_Toc478379025)

[1.2 Related Documents 7](#_Toc478379026)

[2 Business Flow 8](#_Toc478379027)

[2.1 Payment Methods for Transactions: 8](#_Toc478379028)

[2.2 Direct Debit Transaction 10](#_Toc478379029)

[3 Merchant Setup Process 12](#_Toc478379030)

[4 Payment Gateway Test System 14](#_Toc478379031)

[5 Online Payments over the Internet 16](#_Toc478379032)

[5.1 Payment Mode Selection 16](#_Toc478379033)

[5.2 Payment Portal Transactions 17](#_Toc478379034)

[6 Integration with PG – Payment Portal 19](#_Toc478379035)

[6.1 Payment Portal – Input Parameters 19](#_Toc478379036)

[6.1.1 Optional Merchant Defined Fields 22](#_Toc478379037)

[6.1.2 Optional Fields for Member Bank 22](#_Toc478379038)

[6.2 Payment Portal Response 24](#_Toc478379039)

[6.2.1 Optional fields 27](#_Toc478379040)

[6.2.2 Optional Fields from Member Bank 27](#_Toc478379041)

[6.3 Receiving the Transaction Response 27](#_Toc478379042)

[7 Payment Status Inquiry 28](#_Toc478379043)

[7.1 Payment Status Inquiry Input Parameters 28](#_Toc478379044)

[7.2 Payment Status Inquiry Response 29](#_Toc478379045)

[7.3 Payment Status Inquiry Processing 31](#_Toc478379046)

[8 Payment Status Update 32](#_Toc478379047)

[8.1 Update Payment Status Input Parameters 32](#_Toc478379048)

[8.2 Update Payment Status Response 34](#_Toc478379049)

[8.3 Update Payment Status Reiteration 34](#_Toc478379050)

[9 Delivery Status Update 36](#_Toc478379051)

[9.1 Delivery Status Update Input Parameters 36](#_Toc478379052)

[9.2 Delivery Status Update Response Parameters 37](#_Toc478379053)

[9.3 Delivery Status Update Processing 38](#_Toc478379054)

[10 Refund Transaction 40](#_Toc478379055)

[11 Integration with PG Via Payment API 40](#_Toc478379056)

[11.1 Payment API – Input Parameters 40](#_Toc478379057)

[11.2 Payment API – Request Parameters 41](#_Toc478379058)

[11.2.1 Optional Merchant Defined Fields 43](#_Toc478379059)

[11.3 Payment API Response 43](#_Toc478379060)

[11.3.1 Optional fields 46](#_Toc478379061)

[11.3.2 Receiving Payment API Response 46](#_Toc478379062)

[11.4.3 Sample Payment API Request from SOAP UI Tool 47](#_Toc478379063)

[11.4.4 Sample Payment API Response 48](#_Toc478379064)

[12 Calculating and Validating the Secure Hash 49](#_Toc478379065)

[12.1 How the Secure Hash is Created and Verified 49](#_Toc478379066)

[12.2 How is SHA256- HMAC Calculated 50](#_Toc478379067)

[13 Padding Rules 52](#_Toc478379068)

[14 Appendix I – Response Code 53](#_Toc478379069)

[15 Appendix II – Amount Values for Generating Different Response in Test Environment 55](#_Toc478379070)

[16 Appendix III – Fixed Length 57](#_Toc478379071)

# 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)

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.

## 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.

## 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.

# 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:

## Payment Methods for Transactions:

The online user experience will be divided between two portals:

1. Merchant’s Web site
2. PMCL 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

1. **Product Details:** Upon check-out the merchant confirms the items to be purchased
2. **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*

1. **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.

**PMCL 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 or over the counter.

**OR**

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

1. **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.

1. **Over the Counter:**

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

## Direct Debit Transaction

The online user experience will be divided between three portals:

1. Merchant’s Web site
2. PMCL 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

1. **Product Details:** Upon check-out the merchant confirms the items to be purchased
2. **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

1. **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.

**PMCL 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**

1. **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

# Merchant Setup Process

In order to process online payments using the PMCL 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:
   1. Payment Gateway Payment Portal Integration Guide
   2. 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:
   1. **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.

1. 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.
2. 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.
3. 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.
4. 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/Merchant Portal/transactionmanagement/merchantform](http://localhost/Merchant%20Portal/transactionmanagement/merchantform)”

\* In place of localhost test environment IP should be placed

1. 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.

# 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 accidently 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.

# 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.

## 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.
   1. Debit Card
   2. Over the counter
   3. Mobile Wallet
   4. Direct Debit

## 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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

# 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.

## 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:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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:   * 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 | 9th 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. |
| pp\_TxnExpiryDateTime | 14 N | Yes | 9th 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. |
| 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 |  |

### 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.

### 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.

## 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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\_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 | 9th 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\_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 | 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. |
| 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 | 9th 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 | 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\_SecureHash | 64 AN | No | 9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6 | Used to allow the Merchant to check the integrity of the transaction response. |
| 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  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 |  |
| ppmbf\_xxxx | 255 AN | No |  |

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

### 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.

### 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.

## 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.

# 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.

## 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:   * 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. |

## 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 | 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 case a transaction is already confirmed by the merchant. |
| Auth Code | 12 N | No | 123456987456 | 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. |
| Settlement Expiry | 14N | No | 9th 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 field will be mandatory where Auth Code is available. |
| BankID | 4 AN | No | BNK1 | This field will only be used in case of DD transaction type, otherwise it should be sent as an empty field.  Customer’s bank that authorized the transaction. |
| 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. |
| CustomerCardNo | 20 N | No | 987156324000123654789 | As provided in the transaction cycle.  This field will only be sent as emty if the transaction type is OTC/MIGS/Mwallet. |
| Secure Hash | 64 AN | No | 9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6 | Used to allow the Merchant to check the integrity of the transaction request. |

## 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 stae, 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.

# Payment Status Update

Merchant will be required to expose a transaction status update web service for Payment Gateway to update status of voucher 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.

## 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:   * 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 | 9th 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\_RetreivalReferenceNo | 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 | 9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6 | Used to allow the Merchant to check the integrity of the transaction message. |

## 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 | 9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6 | Used to allow the Payment Gateway to check the integrity of the transaction request. |

## 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.

# 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’.

## 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:   * 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 | 9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6 | Used to allow the Payment Gateway to check the integrity of the transaction request. |

## 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 | 9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a4 | Used to allow the Merchant to check the integrity of the response. |

## 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 |

# Refund Transaction

Trasnaction 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.

# 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.

## 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.

## 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 | 9th 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. |
| pp\_TxnExpiryDateTime | 14 N | Yes | 9th 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 | 9e107d9d372bb6826bd81d3542a419d69e107d9d372bb6826bd81d3542a419d6 | 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  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\_5 | 255 AN | No |  |

### 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.

## 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 | 9th 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 | 9th 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 : xxxxxxxxxxx |
| 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 |  |

### 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.

### 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 refere

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.

### 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\_TxnExpiryDateTime>

<tem:pp\_ReturnURL>http://localhost/MerchantSimulator/HttpRequestDemoServer/Index</tem:pp\_ReturnURL> <tem:pp\_SecureHash>5212E6DC8A73E6335663476E9A52CEF9950811815529E8C2F44F7125D0B3E3E2</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>

### 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

# 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.

## 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:

0F5DD14AE2E38C7EBD8814D29CF6F6F0**2995***MER123*A48cvE28

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.

## 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.

1. To this concatenated string, Shared Secret is prepended.
2. This string is first converted into UTF8 bytes and then it is converted into ISO-8859-1 encoding.
3. The ISO-8859-1 string is then hashed using HMAC with UTF-8 encoded Shared Secret as key.
4. 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:

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.

The hash output must be hex-encoded.

# 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 |

# Appendix I – Response Code

|  |  |
| --- | --- |
| **Response Code** | **Response Code Description** |
| 000 | Transaction processed successfully. |
| 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. |
| 157 | Transaction is pending.(for Mwallet and MIgs) |
| 199 | System error |
| 200 | Transaction approved – Post authorization |
| 210 | Authorization pending |
| 999 | Transaction failed. This response code will be sent when the transaction fails due to some technical issue at PG or Bank’s end. |

# 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 |

# 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.