

VERSION 5.1.1

JANUARY 11, 2017



MOBILE MONEY PAYMENT GATEWAY

TECHNICAL DOCUMENTATION

Table of Contents

OVERVIEW	3
COMMUNICATION	3
MESSAGE 1 – REQUEST FROM MERCHANT’S WEBSITE	3
MESSAGE 2 – SUCCESS RESPONSE FROM THE PAYMENT GATEWAY	4
MESSAGE 2 – FAILED RESPONSE FROM THE PAYMENT GATEWAY	5
CONSTRAINTS.....	5
RESPONSE LAYER.....	5
HTTP LAYER RESPONSE	6
RESPONSE REASON CODES:	6

OVERVIEW

Ooredoo Mobile Money Payment Gateway Integration for Mobile Money will facilitate functions and features required to integrate and introduce Merchants with web portals to Mobile Money product line. This document is intended for technical points and all content of this document has technical descriptions.

Customer can visit the merchant shop, purchase goods and pay the money online from his MM wallet. This payment can be done by any Full wallet customers Including Ooredoo and non-Ooredoo (Off-Net). In case of payment by Ooredoo Customer, Customer authentication will be via USSD push authentication and in case of Off-Net customers' authentication will be via OTP which will be sent to customer mobile number during the transaction.

Below is the detailed description of a dummy process:

1. The Customer visits the Merchant's website, retrieves the payment item (for example a bill) and selects to make payment by Mobile Money Payment Gateway.
2. A payment request message is sent by the Merchant's website to the MMOnline Payment Gateway. Refer to *Message 1 – Request from Merchant's Website* for details of this call . The Merchant shall share the requesting and reply URLs with us for authorization.
3. The Payment Gateway verifies the Merchant's details and the integrity of the message received by verifying the hash signature. The Payment Gateway checks for duplicate payments before processing the payment.
4. The Payment Gateway replies to the Merchant's website with a response message. Refer to *Message 2 and Message 3 – Response from the Payment Gateway* for details of the message.

COMMUNICATION

Mobile Money Payment Gateway Integration API will be called only via HTTP, no other protocol is allowed. Irrespective of language request must be a HTTP POST request.

Protocol: HTTP

Method: POST

MESSAGE 1 – REQUEST FROM MERCHANT'S WEBSITE

Merchant has to call the below URL for completing a payment with Mobile Money Online Payment Gateway with parameters mentioned in the table below. All the parameters are compulsory to complete a transaction.

<http://ooredoo.mv/MMOnlinePayment /MobileMoney/verify>

NAME	VALUE
MerID	Merchant Mobile Money enabled phone number.

TxnId	The transaction ID of the order that uniquely identifies the transaction in the Merchant's system. It should be unique for the Merchant.
PayAmt	This is the total amount of the purchase. Payment amount as calculated by the Merchant's system. Payment amount will be of 7 digits. Left padded with 0. Last 2 digits shall be reserved for decimal places.
MerRespURL	The response URL for getting the result back. This is the URL of a web page on Merchant's server where response will be sent. The URL shall be provided for authorization purpose.
Signature	<p>This is a digital signature that will verify that the contents of the request is not altered in transit. A hash signature calculated from the following:</p> <p>(MerID . MerPin . MerKey. TxnId. PayAmt)</p> <ol style="list-style-type: none"> 1. MerID – The Mobile Money enabled no. of Merchant's number. 2. MerPin – The Mobile Money enabled no. of Merchant's pin. 3. MerKey – Merchant identification number provided by Ooredoo. 4. TxnId – Merchant's unique transaction ID per order. 5. PayAmt – The total purchase amount. <p>The hash value that is produced uses SHA1 hash algorithm. Hash has to be generated and sent along with the parameters so as to verify the request is not altered in transit.</p>

Note: The PayAmt is the payment amount, will be only 7 digits in total and left padded with zero's. The last two digits shall be reserved for decimal places. Therefore, the amount 156.97 should be 0015697. And Amount 19.00 should be 0001900 .

MESSAGE 2 – SUCCESS RESPONSE FROM THE PAYMENT GATEWAY

The Response shall be a form request. The success response shall return the success status code, Ooredoo TransactionID, Merchant TransactionID and hash of (status code, Ooredoo TransactionID, Merchant TransactionID and Merchant Key) . Hash is generated so as to verify the message is not altered in transit.

NAME	VALUE
status	The result of the transaction. The code is 1001 always for success.
hash	SHA1 hash of (... status)
transactionID	Ooredoo transaction ID equivalent of Merchant transaction id. This is unique in Ooredoo system issued for each Merchant's transaction ID.

MerchantTxnID	The transaction ID of the order that uniquely identifies the transaction in the Merchant's system. It should be unique for the Merchant.
Signature	<p>The hash value that is produced uses SHA1 hash algorithm . A hash signature calculated from the following: (MerchantTxnID . transactionID . MerKey . status)</p> <ol style="list-style-type: none"> 1. status – The success code for the transaction. i.e 1001 2. MerchantTxnID – Merchant's unique transaction ID per order. 3. transactionID – Ooredoo's unique transaction ID per order. 4. MerKey – Merchant identification number provided by Ooredoo.

Note: *The status for successful transaction will always be 1001.*

MESSAGE 2 – FAILED RESPONSE FROM THE PAYMENT GATEWAY

The Response shall be a form request. The failed response shall return the fail status code, Ooredoo TransactionID, Merchant TransactionID ,and Message for the failure of the transaction.

NAME	VALUE
status	The result of the transaction. The code is 1001 always for success.
transactionID	Ooredoo transaction ID equivalent of Merchant transaction id. This is unique in Ooredoo system issued for each Merchant's transaction ID.
MerchantTxnID	The transaction ID of the order that uniquely identifies the transaction in the Merchant's system. It should be unique for the Merchant.
message	Description of why the transaction failed.

CONSTRAINTS

API is expected to fail when there is a TCP communication gap between third party system and Ooredoo Maldives.

Except above case all are well handled and communicated via HTTP Responses.

RESPONSE LAYER

Response layer will cover response types and method of the response types. The Success response are returned as a form request.

HTTP LAYER RESPONSE

HTTP responses are considered as fail responses where third party might not be able to connect to Ooredoo Maldives application programming interface for several reasons such as network access or firewall blocking.

- Native HTTP Response Format

Below are all the Error Codes, which would be given in case of the reason as mentioned below:

RESPONSE REASON CODES:

Error Code	Description
1001	Successful transaction.
4001	Unauthorized transaction.
4002	Incomplete Information.
2004	Internal fault or exception
10331	Transaction id is required
10537	Merchant is not registered in MM
10538	Customer is not registered in MM
10539	OTP is required.
10301	No configuration found for this hierarchy
2611	Sender does not have sufficient balance.
2563	Payee exceed monthly limit
2564	Payer exceed monthly limit
2565	Payee exceed daily limit
2566	Payer exceed daily limit
2567	Payee exceed weekly limit
2568	Payer exceed weekly limit
2594	Payee exceed the monthly limit count
2595	Payer exceed the monthly limit count
2596	Payee exceed the daily limit count
2597	Payer exceed the daily limit count
329	Credential did not match
10335	Customer did not respond the pin with in timeout (For Ussd Message)
10540	Merchant mobile number is required.
10541	Customer mobile number is required.
10542	Merchant mobile number is invalid format.
10543	Customer mobile number is invalid format.
51	Trace number should not be duplicate
1008	User is blacklisted