belize bank
Our Country. Your Bank

BELIZE BANK LIMITED CARD PAYMENT GATEWAY

Integration Guide

November 14, 2023
Version 1.3

TABLE OF CONTENTS

CONFIDENTIALITY

The information herein is confidential and proprietary. No disclosure, reproduction, or further dissemination of this document may be made without the express written consent of The Belize Bank Limited.

HISTORY

Version	Date	Description
1.0	March 25, 2022	Initial document
1.1	April 27, 2022	Removal of certain features
1.2	May 10, 2022	Include tokenization feature
1.3	November 14, 2023	Including additional information in various sections

INTRODUCTION

Purpose

This document contains the specifications to integrate to the Belize Bank Limited Card Payment Gateway. This gateway is used by the Bank to process credit and debit card payments on behalf of a merchant registered with the Belize Bank.

It must be noted no information contained in this document at any point supersedes the policies and procedures set forth in the Bank's Merchant Guidelines agreement, nor the regulations set forth by Visa and Mastercard.

Audience

The primary audience of this document are software developers.

SYSTEM ARCHITECTURE

Overview

The Belize Bank Card Payment Gateway is a service available to merchants of the Belize Bank to process card payments via a merchant's system, more specifically a website or mobile app, in a completely automated fashion.

Communication with the Belize Bank Card Payment Gateway is done via REST based web services. All requests will be sent as POST requests in application/x-www-form-urlencoded content type format. All responses will be sent as JSON objects in the application/json content type format. This provides an operating system, programming language, and hardware platform independent interface.

Access to a test environment will be provided. Merchants must be able to demonstrate successful integration with the Belize Bank Card Payment Gateway test environment before being allowed to connect to the production environment of the same.

The URL and credentials to connect to the test and production environment will be provided outside of this document. The specifications provided below remain the same regardless of the environment being connected to; and will be indicated by the placeholder `{payment-url}`.

Integration is performed using the hosted payment page concept.

Hosted Payment Page

Using the hosted payment page concept, the card information will be entered and processed entirely on the Belize Bank Card Payment Gateway server.

This method does not require the merchant's system to be PCI DSS compliant.

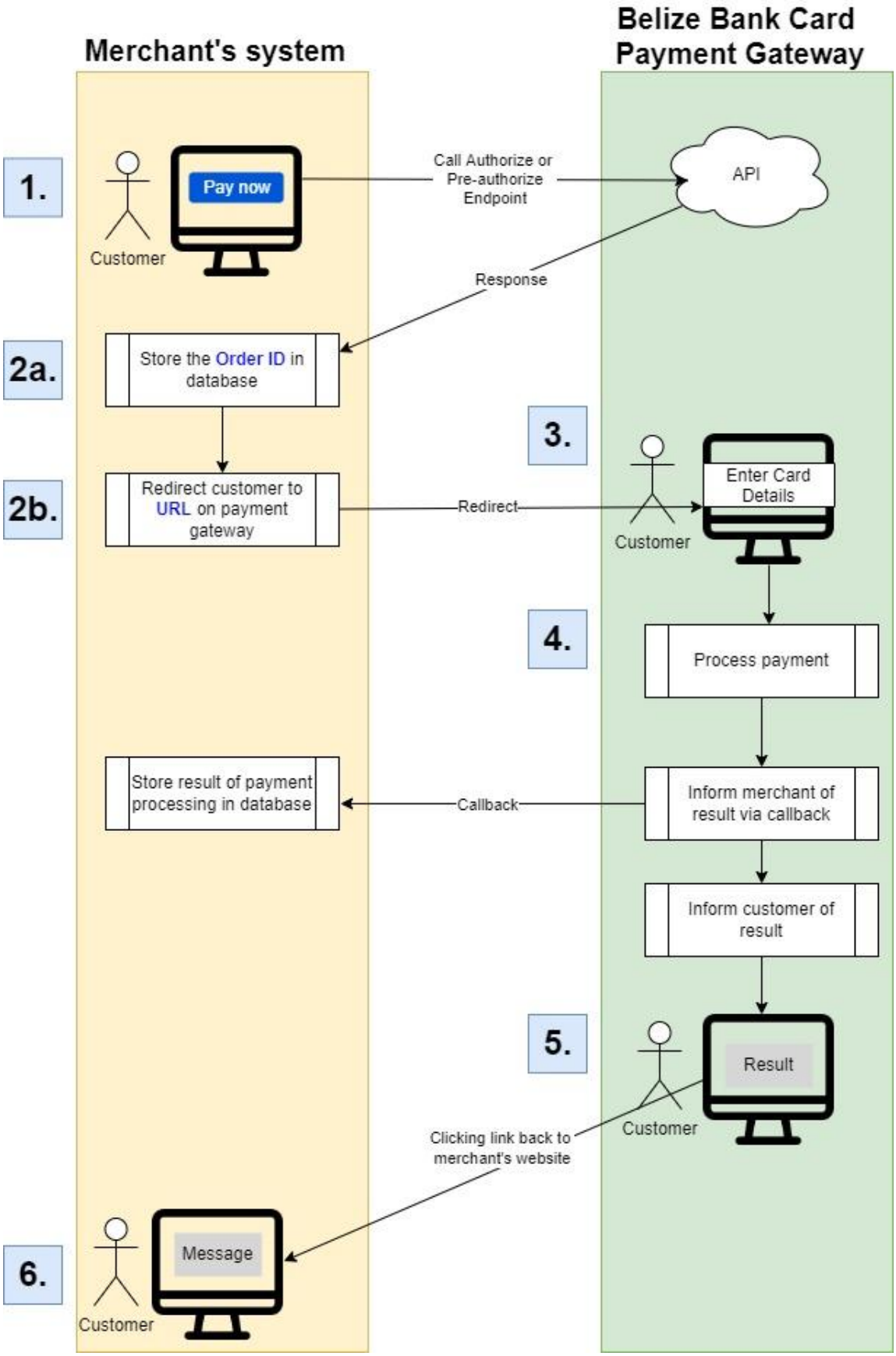
This service completely removes the need for the merchant to store in its own systems any information related to the credit or debit card of its clients. The Bank therefore strongly recommends the merchant to refrain from storing any such card information on its systems. This reduces the risk of unauthorized disclosure of payment card information.

The flow between the merchant's website and the payment gateway is as follows:

1. When a customer is ready to perform payment, the merchant's website must call the authorization or pre-authorization endpoint
2. This endpoint in its response will return:

    a. an order ID which must be stored in the merchant's system
    b. A URL to a page hosted on the payment gateway to which the customer must be redirected
3. The customer will now enter the card information on this page
4. The payment gateway will process the payment and can optionally inform the merchant's system of the result via a callback function
5. The payment gateway will also inform the customer of the result of the processing of the payment
6. The page containing the result of the payment will also contain a link to direct the customer back to the merchant's website

A diagram of this flow is shown below


Merchant's system
Belize Bank Card Payment Gateway
1.
Pay now
Customer
Call Authorize or Pre-authorize Endpoint
API
Response
2a.
Store the Order ID in database
2b.
Redirect customer to URL on payment gateway
Redirect
3.
Customer
Enter Card Details
4.
Process payment
Store result of payment processing in database
Callback
Inform merchant of result via callback
Inform customer of result
5.
Result
Customer
Clicking link back to merchant's website
6.
Message
Customer

Authentication

Each merchant will be provided with a username and password which must be used when sending a request to the payment gateway. It is the responsibility of the merchant to safeguard these credentials.

Postman Collection

A Postman collection is available for download and use for testing all endpoints of the payment gateway. This Postman collection can be downloaded here.

There are 3 variables defined in the Postman collection that must be set before calling any endpoint: `server`, `username`, and `password`. The values to place in these variables will be discussed below.

Test Credentials

The value to place in the `server` variable when calling an API endpoint in the Bank's test environment will always be `https://sandbox.belizebank.com/payment/rest`

The value to place in the `username` and `password` variables when calling an API endpoint in the Bank's test environment will be provided by the Bank when the merchant is ready to test the integration.

The following card numbers can be used when performing transactions in the test environment.

Card Number	Expiration Date	CVC	Expected Result
4000001111111118	12/30	123	Successful transaction
4111111111111111	12/24	123	Successful transaction
4444444411111111	12/24	123	Declined
5555555555555599	12/24	123	This transaction will be subject to 3DS authentication.

Production Credentials

The value to place in the `server` variable when calling an API endpoint in the production environment will always be `https://gateway.belizebank.com/payment/rest`

The value to place in the `username` and `password` variables when calling an API endpoint in the Bank's production environment will be provided by the Bank when the merchant is ready to launch the integration. These values are sensitive and must be handled as such.

PAYMENT AUTHORIZATION ENDPOINT

Purpose: This endpoint must be used by the merchant's system to accept and process a payment being made by its customer.

URL: `{payment-url}`/register.do

Request Body:

Field name	Use	Description
userName	Mandatory	This is the user name. It is used to authenticate the origin of the request message.
password	Mandatory	This is the password. Used to authenticate the origin of the request message.
amount	Mandatory	The amount of the transaction. The amount must be 2 decimal places implied. For example $45.00 must be sent as 4500
description	Optional	A description of the goods or services being purchased associated with the payment.
returnURL	Mandatory	This is the URL the merchant will be redirected to upon clicking the "Return to Merchant" link in the page showing the result of the payment.
orderNumber	Optional	This is the unique identifier of this payment in the merchant's system. You cannot submit multiple payment requests with the same order number.
clientId	Optional	This is the unique identifier of the merchant's customer in the merchant's system. This value is used as part of the tokenization feature to link a saved card to a customer. **Extreme care** must be used when populating this field to ensure a saved card for one customer is not shown to another customer.
email	Optional	The email of the customer performing the payment. If specified, the payment gateway will send an email receipt of the payment performed to this specified email address.
dynamicCallbackUrl	Optional	The URL on the merchant's system that will be called by the card payment gateway to inform the merchant of an event on this authorization.

billingPayerData	Optional	The billing address of the cardholder, used for the address verification service (AVS) check. The format of this field is defined in the Appendix.

Request Example:

```
(
   "userName":"testuser",
   "password":"testpassword",
   "amount":4500,
   "description":"Order #52. Hollister Shirt.",
   "returnURL":"https://merchant-website.com",
)
```

Response Body:

Field name	Description
orderID	Order ID of this payment in the card payment gateway. This value must be stored in the merchant's system as it is used when performing related actions for this payment such as reversals, refunds, inquiring about the payment status, and handling the callback messages.
formURL	The URL of the payment page on the payment gateway the merchant's system needs to direct its customer to.
errorCode	This field will only be present if the endpoint call was unsuccessful. It will contain a code to help identify the reason for the error.
errorMessage	This field will only be present if the endpoint call was unsuccessful. It will contain a description of the error.

Successful Response Example:

```
{
   "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
formURL":"https://gateway-website.com/payment.html?mdOrder=669e55c4
-f72b-729c-be53-b7e100b0b260&language=en",
}
```

Unsuccessful Response Example:

```
{
   "errorCode":4,
   "errorMessage":"The amount field is empty",
}
```

PAYMENT PRE-AUTHORIZATION ENDPOINT

Purpose: This endpoint must be used by the merchant's system to process a pre-authorization on the card. This endpoint will not charge the card but place a hold so a charge can be placed later when the final payment amount is known. This pre-authorization can subsequently be converted to a charge on the account using the pre-authorization capture endpoint.

Note preauthorizations have an expiration date as to how long they remain on a card. Preauthorizations are released if not converted to an authorization within a specified period. The expiration date of the preauthorization depends on the card issuer, but usually varies between 2 weeks to 1 month from the time the preauthorization was initially approved.

URL: `{payment-url}`/registerPreAuth.do

Request Message Body:

Field name	Use	Description
userName	Mandatory	This is the user name. It is used to authenticate the origin of the request message.
password	Mandatory	This is the password. Used to authenticate the origin of the request message.
amount	Mandatory	The amount of the transaction. The amount must be 2 decimal places implied. For example $45.00 must be sent as 4500
description	Optional	A description of the goods or services being purchased associated with the payment.
returnURL	Mandatory	This is the URL the merchant will be redirected to upon clicking the "Return to Merchant" link in the page showing the result of the payment.
orderNumber	Mandatory	This is the unique identifier of this order in the merchant's system. You cannot submit multiple authorization requests with the same order number.
clientId	Optional	This is the unique identifier of the merchant's customer in the merchant's system. This value is used as part of the tokenization feature to link a saved card to a customer. **Extreme care** must be used when populating this field to ensure a saved card for one customer is not shown to another customer.

email	Optional	The email of the customer performing the payment. If specified, the payment gateway will send an email receipt of the payment performed to this specified email address.
dynamicCallbackUrl	Optional	The URL on the merchant's system that will be called by the card payment gateway to inform the merchant of an event on this pre-authorization.
billingPayerData	Optional	The billing address of the cardholder, used for the address verification service (AVS) check. The format of this field is defined in the Appendix.

Request Message Example:

```
(
   "userName":"testuser",
   "password":"testpassword",
   "amount":4500,
   "orderNumber": 123456,
   "description":"Order #52. Hollister Shirt.",
   "returnURL":"https://merchant-website.com",
)
```

Response Message Body:

Field name	Description
orderID	Order ID of this payment in the payment gateway. This value must be stored in the merchant's system as it is used when performing related actions for this payment such as pre-authorization captures, reversals, refunds, inquiring about the payment status, and handling the callback messages.
formURL	The URL of the payment page on the payment gateway the merchant's system needs to direct its customer to.
errorCode	This field will only be present if the endpoint call was unsuccessful. It will contain a code to help identify the reason for the error.
errorMessage	This field will only be present if the endpoint call was unsuccessful. It will contain a description of the error.

Successful Response Message Example:

```
{
   "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
```

```
formURL":"https://gateway-website.com/payment.html?mdOrder=669e55c4
-f72b-729c-be53-b7e100b0b260&language=en",
}
```


Unsuccessful Response Message Example:


```
{
   "errorCode":4,
   "errorMessage":"The amount field is empty",
}
```

PRE-AUTHORIZATION CAPTURE ENDPOINT

Purpose: This endpoint must be used when settling a pre-authorization performed using the payment pre-authorization endpoint; and converting said pre-authorization to a charge on the card.

URL: `{payment-url}`/deposit.do

Request Body:

Field name	Description	Detail
userName	Mandatory	This is the user name. It is used to authenticate the origin of the request message.
password	Mandatory	This is the password. Used to authenticate the origin of the request message.
orderId	Mandatory	This must be the same the order ID obtained in the response message of the pre authorization endpoint
amount	Mandatory	This is the amount to charge to the card. The amount must be 2 decimal places implied. For example $45.00 must be sent as 4500. The maximum amount that can be charged to the card using the pre-authorization capture must adhere to Visa and Mastercard regulations.

Request Body Example:

```
(
   "userName":"testuser",
   "password":"testpassword",
   "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
   "amount":4525
)
```

Response Message Body:

Field name	Description
errorCode	A code indicating if the endpoint call was successful. A value of 0 means the call was successful. Any other value means the call was not successful.

errorMessage	This field will contain a description of the error if the endpoint call was unsuccessful.

Successful Response Message Example:

```
{
   "errorCode":0,
   "errorMessage":"Success",
}
```

Unsuccessful Response Message Example:

```
{
   "errorCode":5,
   "errorMessage":"Deposited amount is exceeding approved amount",
}
```

REVERSAL ENDPOINT

Purpose: This endpoint can be used to void or reverse a payment. A payment can only be voided or reversed if it has not been settled.

URL: `{payment-url}`/reverse.do

Request Body:

Field name	Description	Detail
userName	Mandatory	This is the user name. It is used to authenticate the origin of the request message.
password	Mandatory	This is the password. Used to authenticate the origin of the request message.
orderId	Mandatory	This must be the same order ID obtained in the response message of the authorization or pre authorization endpoint.

Request Body Example:

```
(
   "userName":"testuser",
   "password":"testpassword",
   "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
)
```

Response Message Body:

Successful Response Message Example:

```
{
    "errorCode": "0",
    "errorMessage": "Success",
}
```

Unsuccessful Response Message Example:

```
{
   "errorCode":7,
```

```
   "errorMessage":"Reversal is impossible for current transaction
state",
}
```

REFUND ENDPOINT

Purpose: This endpoint can be used to perform a refund. A payment can only be refunded after it has been settled. A refund must be associated with a previously processed payment and can be partial or in full but cannot at any point exceed the amount of the related payment.

URL: `{payment-url}`/refund.do

Request Body:

Field name	Description	Detail
userName	Mandatory	This is the user name. It is used to authenticate the origin of the request message.
password	Mandatory	This is the password. Used to authenticate the origin of the request message.
orderId	Mandatory	This must be the same order ID obtained in the response message of the authorization or pre authorization endpoint.
amount	Mandatory	The amount of the refund. The amount must be 2 decimal places implied. For example $45.00 must be sent as 4500

Request Body Example:

```
(
   "userName":"testuser",
   "password":"testpassword",
   "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
   "amount":4500
)
```

Response Message Body:

Successful Response Message Example:

```
{
    "errorCode": "0",
    "errorMessage": "Success",
}
```

Unsuccessful Response Message Example:

```
{
   "errorCode":7,
   "errorMessage":"Refund is impossible for current transaction
state",
}
```

PAYMENT STATUS ENDPOINT

Purpose: This endpoint can be used to obtain the status of a payment.

URL: `{payment-url}`/getOrderStatusExtended.do

Request Body:

Field name	Description	Detail
userName	Mandatory	This is the user name. It is used to authenticate the origin of the request message.
password	Mandatory	This is the password. Used to authenticate the origin of the request message.
orderId	Mandatory	This must be the same the order ID obtained in the response message of the authorization or pre authorization endpoint

Request Body Example:

```
(
   "userName":"testuser",
   "password":"testpassword",
   "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
)
```

Response Message Body:

Field name	Description
errorCode	A code indicating if the endpoint call was successful. A value of 0 means the call was successful. Any other value means the call was not successful.
errorMessage	Error Message. This field will contain a description of the error if the endpoint call was unsuccessful.
orderStatus	The status of the transaction. It can have the possible following values: ● 0 - transaction was registered but not paid ● 1 - pre-authorized amount is on hold on the buyer's account (for two-phase payments) ● 2 - transaction amount is fully authorized ● 3 - transaction canceled

	● 4 - transaction refunded ● 5 - access control server of the issuing bank initiated authorization procedure ● 6 - authorization declined
date	The date and time the transaction was initiated in epoch. For example a value of 1648501318153 means Mon Mar 28 2022 15:01:58 GMT-06:00
refundedDate	The date and time the transaction was partially or fully refunded. In the scenario of multiple partial refunds, this field contains the date and time of the most recent refund.
authDateTime	The date and time the transaction was authorized.
ip	The IP address from where the merchant's customer initiated the transaction
bindingID	The tokenized value of the card used if the cardholder decided to save his card on the card payment gateway for future use. This value must be saved by the merchant in its system in order to perform subsequent transactions with the same card.
cardAuthInfo	This is a parent tag. The child fields are below.
->maskedPan	The card number in masked form used to perform the transaction. For example 555555**5599
->cardholderName	The name entered when performing the transaction.
->approvalCode	The approval code issued for this transaction.

Successful Response Message Example:

```
{
    "errorCode": "0",
    "errorMessage": "Success",
    "orderStatus": 4,
    "amount": 4500,
    "date": 1648501318153,
    "refundedDate": 1648501672000,
    "ip": "179.42.221.32",
    "cardAuthInfo": {
        "maskedPan": "555555**5599",
        "cardholderName": "JOHN TEST",
        "approvalCode": "123456",
    },
```

```
}
```

Unsuccessful Response Message Example:

```
{
   "errorCode":6,
   "errorMessage":"Order not found",
}
```

PAYMENT VIA TOKENIZED CARD ENDPOINT

Purpose: This endpoint can be used to perform an authorization or pre-authorization using a tokenized card.

URL: `{payment-url}`/paymentOrderBinding.do

Request Body:

Field name	Description	Detail
userName	Mandatory	This is the user name. It is used to authenticate the origin of the request message.
password	Mandatory	This is the password. Used to authenticate the origin of the request message.
mdOrder	Mandatory	This must be the orderID returned from the authorization or pre-authorization endpoint. Note this authorization or pre-authorization must be created specifying the same value in the client ID field specified used to obtain the bindingID below.
bindingID	Mandatory	This must be the bindingID returned from the payment status endpoint

Request Body Example:

```
(
   "userName":"testuser",
   "password":"testpassword",
   "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
   "bindingID":"9ca72329-f228-7b6b-81c2-032e00b0b260",
)
```

Response Message Body:

Field name	Description
errorCode	A code indicating if the endpoint call was successful. A value of 0 means the call was successful. Any other value means the call was not successful.
errorMessage	Error Message. This field will contain a description of the error if the

	endpoint call was unsuccessful.
redirect	The URL of a page on the card payment gateway that can be shown to the cardholder indicating the payment was successful
info	An optional message that can be shown to the cardholder
bindingID	The bindingID sent in the request message

Successful Response Message Example:


```
{
"redirect":"https://sandbox.radarpayment.online/payment/merchants/ecom/finish.html?orderId=367ad754-1c27-778a-a109-7f6d00b0b260&lang=en",
   "info":"Your order is proceeded, redirecting...",
   "errorCode":0,
   "bindingId":"9ca72329-f228-7b6b-81c2-032e00b0b260"
}
```


Unsuccessful Response Message Example:


```
{
   "error":"No order found",
   "errorCode":2,
   "errorMessage":"No order found"}
}
```

CALLBACK ENDPOINT

Purpose: This endpoint can be used by the merchant's system to be informed when an event has occurred on a previously submitted authorization or pre-authorization on the Belize Bank Card Payment Gateway.

This endpoint must be accessible on the merchant's system via a HTTP post method. The response will be provided in the application/x-www-form-urlencoded content type format.

A callback is triggered when any of the following actions occur on a authorization or pre-authorization:

- A pre-authorization has been approved
- An authorization has been approved
- A pre-authorization has been captured
- An authorization has been reversed or voided
- A refund has occurred

URL: Value provided in the dynamicCallBackUrl field in the authorization or pre-authorization request

Request Body:
Not applicable

Response Body:

Field name	Description	Detail
mdOrder	Mandatory	The order ID assigned to this payment by the card payment gateway. This corresponds to the orderID field in the pre-authorization and authorization response.
orderNumber	Mandatory	An order number assigned to this payment by the card payment gateway. Its use is optional.
operation	Mandatory	The operation which triggered the callback. The possible values for this field are defined in the Appendix.
status	Mandatory	The status of the transaction. A value of 1 means success.

Successful Response Message Example:

```
orderNumber=65436&mdOrder=2593e67b-f5cc-7fc3-a85d-98f400b0b260&operation=deposited&status=1
```

APPENDIX

Format of billingPayerData object

Field name	Mandatory	Description
billingCity	Yes	The city registered on a specific card of the Issuing Bank.
billingCountry	No	The country registered on a specific card of the Issuing Bank (ISO 3166-1, numeric).
billingAddressLine1	No	The address registered on a specific card of the Issuing Bank. Line 1.
billingAddressLine2	No	The address registered on a specific card of the Issuing Bank. Line 2.
billingAddressLine3	No	The address registered on a specific card of the Issuing Bank. Line 3.
billingPostalCode	Yes	Postal code registered on a specific card of the Issuing Bank.
billingState	No	The state registered on a specific card of the Issuing Bank (ISO 3166-2).

Example of object: {"billingCity":"City", "billingPostalCode":"12345"}

List of values for operation field

Value	Comment
approved	Used when a pre-authorization has been approved
deposited	Used when an authorization has been approved, or a pre-authorization has been captured
reversed	Used when an authorization has been reversed or voided
refunded	Used when a refund has occurred