KINA BANK LIMITED

ECOMMERCE MERCHANT INTEGRATION GUIDE

Version 1.5

Document Information

Prepared By	: Kina Bank Limited	Document Version No	: 1.5
		Document Version Date	: 18 Nov 2020

Version History

Ver. No.	Ver. Date	Revised By	Description	Remarks
1.0	23 Jun 2020	Tan Kah Hoe	Initial Document	
1.1	24 Jun 2020	Tan Kah Hoe	Revised Document	Switch term "checkout page" to "order confimation page" Add section for MAC Calculation
1.2	29 Jun 2020	Tan Kah Hoe	Revised Document	Reshuffle MAC source string order Secret Key for HMAC Testing in TEST environment
1.3	30 Jun 2020	Tan Kah Hoe	Revised Document	List of Action Code in Response List of EGW Response Code (RC)
1.4	25 Sep 2020	Tan Kah Hoe	Revised Document	Bank Transfer - OnClick JS function to invoke Bank Transfer page Bank Transfer - New RC -97, -98, -99
1.5	18 Nov 2020	Tan Kah Hoe	Revised Document	Refund w/o Card

Table of Contents

Introduction

This document illustrates the essentials steps to integrate/connect merchant e-commerce website to Kina Payment Gateway.

Kina Payment Gateway support the acceptance of the following Card brands:
1. Visa
2. MasterCard
3. Union Pay (coming soon)

Transaction Flows

1. **Checkout Page**
    After selecting good and services, customer proceed to checkout page to fill in delivery info.

2. **Order confirmation page**.
    Upon finalizing delivery info, customer click a button and merchant site display order confirmation page and present payment method to customer.

3. **Kina Payment Page iframe**
    In order confirmation page, customer choose to pay by credit/debit card. **Order confirmation page** must include a HTTP FORM element that contains INPUT or HIDDEN fields (complete set of fields described in next section) required to authorize the transaction, submit HTML FORM to iframe, FORM target=https://devegateway.kinabank.com.pg/cgi-bin/cgi_link.

    3.1 A page to collect credit card details (hosted by Kina Bank Limited) will be displayed as overlay iframe on top of order confirmation page

4. **Customer click pay**
    In Kina Payment Page iframe, customer fill in card number and other card details, and click pay. Kina payment gateway receive the authorization request and validates request information including the message authentication code (MAC). If the request fails, gateway sends an error response back to merchant system.

5. **Cardholder authentication**.
    If the provided card number belongs to a card range with a defined cardholder authentication method, gateway calls the corresponding authentication module like 3-D Secure, which performs protocol-specific processing like One Time Password. If cardholder authentication is unsuccessful, Gateway returns an error message to the merchant system.

6. **Transaction authorization**
    Gateway sends an authorization request to Kina card system. Upon authorization, reception gateway prepares and sends a transaction response back to the merchant system. If authorization is successful, the response message will contain "Internal Reference Number" field, to be used by the merchant system so it can reverse/refund the obtained authorization without the credit card information.

Authorization Request

Following fields set will be posted to Kina Payment Gateway through HTTP POST method. These fields can be rendered as HTML INPUT or HIDDEN elements in order confirmation page. Merchant site should perform basic prevalidation to ensure the values conform to the below requirements

Field	Size	Description
AMOUNT	1-12	Order amount in float format with decimal point separator, up to 2 decimal point. Example: **98.30**
CURRENCY	03	Order currency: 3-character currency code
ORDER	6-20	Merchant order ID, numeric. Last 6 digits used as a system trace audit number, which must be unique within a day for the terminal id.
DESC	1-50	Order description
MERCH_NAME	1-50	Merchant name (recognizable by cardholder)
MERCH_URL	1-250	Merchant primary web site URL
MERCHANT	15	Merchant ID assigned by bank
TERMINAL	8	Merchant Terminal ID assigned by bank
EMAIL	80	E-mail address for notification. If this field is present Gateway may send transaction results notification to specified e-mail address
TRTYPE	1	Must be equal to "1" (Retail Financial Request).
COUNTRY	02	Merchant shop 2-character country code. Must be provided if merchant system located in a country other than the gateway server's country.
MERCH_GMT	1-5	Merchant UTC/GMT time zone offset (e.g. –3). Must be provided if merchant system located in a time zone other than the gateway server's time zone.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between merchant server and e-Gateway server must not exceed 1 hour, otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
BACKREF	1-250	Merchant URL for posting authorization result.
P_SIGN	1-256	Merchant MAC in hexadecimal form.

Authorization Response

Kina Payment Gateway processes the authorization request and returns the response to merchant URL provided in the **BACKREF** incoming field. Additionally, the same field set may be sent to the merchant via to the email address provided in the **EMAIL** incoming field.

Field	Size	Description
TERMINAL	8	Echo from the request
TRTYPE	2	Echo from the request
ORDER	6-20	Echo from the request
AMOUNT	12	Amount authorized. Usually, will be equal to original amount plus acquirer fee.
CURRENCY	3	Echo from the request
ACTION	1	E-Gateway action code: 0 – Transaction successfully completed; 1 – Duplicate transaction detected; 2 – Transaction declined; 3 – Transaction processing fault; 4 – Information message.
RC	02	Transaction response code (ISO-8583 Field 39)
APPROVAL	06	Client bank's approval code (ISO-8583 Field 38). Can be empty if not provided by card management system.
RRN	12	Merchant bank's retrieval reference number (ISO-8583 Field 37).
INT_REF	1-32	E-Commerce gateway internal reference number
TIMESTAMP	14	E-Commerce gateway timestamp in GMT: YYYYMMDDHHMMSS
NONCE	1-64	E-Commerce gateway nonce value. Will be filled with 8-32 unpredictable random bytes in hexadecimal format. Will be present if MAC is used.
P_SIGN	1-256	E-Commerce gateway MAC (Message Authentication Code) in hexadecimal form. Will be present if MAC is used.

Reversal Request

The reversal transaction request shall be sent by the merchant system Kina Payment Gateway to cancel previously authorized or completed transactions.

All fields are provided by merchant system and the cardholder does not participate in this transaction.

Field	Size	Description
ORDER	6-20	Merchant order ID from request.
AMOUNT	12	Transaction amount. Float format with decimal point separator.
CURRENCY	3	Currency name. Must be the same as in authorization response.
RRN	12	Retrieval reference number from authorization response.
INT_REF	1-32	Internal reference number from authorization response.
TRTYPE	2	Must be equal to "24" (Reversal Request).
TERMINAL	8	Merchant terminal ID assigned by bank. Must be equal to "TERMINAL" field from authorization request.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between Internet shop and e-Gateway must not exceed 1 hour otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
P_SIGN	1-256	Merchant MAC in hexadecimal form.

Reversal Response

Gateway processes a reversal request and returns the result fields to the merchant system within a response document. Response fields and format are the same as for the authorization response.

Purchase Return w/o Card – TRTYPE 174

The reversal transaction request shall be sent by the merchant system Kina Payment Gateway to cancel previously authorized or completed transactions.

All fields are provided by merchant system and the cardholder does not participate in this transaction.

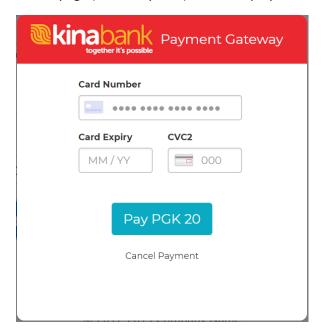| Field	Size	Description
ORDER	6-20	Merchant order ID from request.
AMOUNT	12	Transaction amount. Float format with decimal point separator.
CURRENCY	3	Currency name. Must be the same as in authorization response.
RRN	12	Retrieval reference number from authorization response.
INT_REF	1-32	Internal reference number from authorization response.
TRTYPE	2	Must be equal to "174" (Purchase Return w/o Card).
TERMINAL	8	Merchant terminal ID assigned by bank. Must be equal to "TERMINAL" field from authorization request.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between Internet shop and e-Gateway must not exceed 1 hour otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
P_SIGN	1-256	Merchant MAC in hexadecimal form.

Purchase Return w/o card Response

Response fields and format are the same as the authorization response.

Kina Payment Page Integration

When customer choose to pay by credit/debit card, the following Kina Payment Page a.k.a. card details page (hosted by Kina) will be displayed as overlay iframe on top of order confirmation page

Therefore, it's mandatory to include the following HTML elements in order confirmation page

HTML elements in Merchant Order Confirmation Page

In the <head> section of the order confirmation page HTML

```
<head>
        <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
        <meta http-equiv="Pragma" content="no-cache" />
        <meta http-equiv="Expires" content="0" />
        <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
        <script src="https://devegateway.kinabank.com.pg/kina/js/kbl-ec.js"></script>
        <link href="https://devegateway.kinabank.com.pg/kina/css/kbl-ec.css" rel="stylesheet">
</head>
```

Cache-Control, Pragma and Expires meta tag ensure the page and its content are not cached, use of these meta elements are strongly recommended, these directive will ensure the browser to fetch a fresh copy of the page resources (CSS, JS and Images) from the server rather than using the cache version, which may be outdated.

Viewport meta, it's recommeded to use this tag for fluid and responsive design that looks good in both desktop and mobile

kbl-ec.js and kbl-ec.css are mandatory javascript and css to support the functions and the look and feel of the payment page integration

In the <body> of the checkout page HTML

```
<body>

    <form id="kblPaymentForm" action="https://devegateway.kinabank.com.pg/cgi-bin/cgi_link"
method="POST" target="kblpaymentiframe">
        <input type="text"…/>
        <input type="hidden"…/>
    </form>

    <button type="button" onclick="submitPaymentForm('card')"> Pay by Cards</button>

    <button type="button" onclick="submitPaymentForm('bank')"> Pay by Bank Transfer</button>

    <div id="kbliframediv" class="kbliframeoverlay">
        <div id="kbliframeinnerdiv">
            <iframe id="kblpaymentiframe" name="kblpaymentiframe"></iframe>
        </div>
    </div>

</body>
```

<FORM> tag should enclose all the INPUT fields described in Authorization Request, it's advisable to disable the edit of all fields in order confirmation page and the MAC is precalculated in the P_SIGN fields.

FORM action points to Kina Payment Gateway URL - https://devegateway.kinabank.com.pg/cgi-bin/cgi_link and FORM target points to the id of the iframe

<Button> with onclick event that call the javascript **submitPaymentForm()** to invoke and make the iframe visible. It's recommended for the merchant site to perform prevalidation before displaying the order confirmation page so the values in the INPUT/HIDDEN elements conform to the requirements of Kina Payment Gateway.

<Iframe> is the container for the Kina Payment Page a.k.a Card Details Page

MAC in Request P_SIGN field

The fields used in MAC Generation are dependent on Transaction Type defined in the following table

MAC fields mapping table

TRTYPE	Fields for MAC Generation
1 – Retail Financial Request	TERMINAL TRTYPE AMOUNT CURRENCY ORDER MERCHANT EMAIL BACKREF TIMESTAMP MERCH_NAME COUNTRY MERCH_URL MERCH_GMT DESC NONCE
24 – Reversal Request	ORDER
174 – Purchase Return w/o Card	ORDER

In order to generate or verify the message authentication field, merchant system must assemble a MAC source string; all field values are prefixed with the decimal field length in ASCII and concatenated in a specified order defined in above MAC Fields Mapping Table. If the field is not present, the '-' character is added to the message in its place.

Suppose we have a transaction of following values

Field	Length	Value
TERMINAL	8	99999999
TRTYPE	1	1
AMOUNT	5	11.48
CURRENCY	3	USD
ORDER	6	771446
MERCHANT	15	123456789012345
EMAIL	19	pgw@mail.sample.com
BACKREF	33	https://www.sample.com/shop/reply
TIMESTAMP	14	20030105153021
MERCH_NAME	17	Books Online Inc.
COUNTRY	0	
MERCH_URL	14	www.sample.com
MERCH_GMT	0	
DESC	16	IT Books. Qty: 2
NONCE	16	F2B2DD7E603A7ADA

MAC source string for the above example is:

899999999911511.483USD6771446151234567890123451 9pgw@mail.sample.com33https://www
.sample.com/shop/reply142003010515302117Books Online Inc.-14www.sample.com-16IT
Books. Qty: 216F2B2DD7E603A7ADA

After the MAC source string is assembled, the merchant system must apply a cryptographic
algorithm to generate the message authentication code. The default MAC algorithm is
HMAC_SHA256.

Below is **secret key** (hex encoded) for integration testing in the TEST environment:

debdd135e436905c7a02f20c56c83a4c501adf555457f0df

Secret key for Production will be provided by the bank representative in a secure manner.

Generated MAC result should be sent in "P_SIGN" field, value can be either upper case or lower-case
hexadecimal string.

MAC in Response P_SIGN field

If MAC is sent in the request, MAC will be calculated against the response and store in the P_SIGN field in the response. It's recommended for the merchant to validate the MAC to confirm the integrity of the response data.

For Retail Financial Advice (TRTYPE=1) The source string for response MAC calculation are in the following orders:

Field	Size	Description
ACTION	1	E-Gateway action code: 0 – Transaction successfully completed; 1 – Duplicate transaction detected; 2 – Transaction declined; 3 – Transaction processing fault; 4 – Information message.
RC	02	Transaction response code (ISO-8583 Field 39)
APPROVAL	06	Client bank's approval code (ISO-8583 Field 38). Can be empty if not provided by card management system.
CURRENCY	3	Echo from the request
AMOUNT	12	Amount authorized. Usually, will be equal to original amount plus acquirer fee.
TERMINAL	8	Echo from the request
TRTYPE	2	Echo from the request
ORDER	6-20	Echo from the request
RRN	12	Merchant bank's retrieval reference number (ISO-8583 Field 37).
TIMESTAMP	14	E-Commerce gateway timestamp in GMT: YYYYMMDDHHMMSS
INT_REF	1-32	E-Commerce gateway internal reference number
NONCE	1-64	E-Commerce gateway nonce value. Will be filled with 8-32 unpredictable random bytes in hexadecimal format. Will be present if MAC is used.

EGW Response Code

RC	Description
-1	A mandatory request field is not filled in
-2	CGI request validation failed
-3	Acquirer host (NS) does not respond or wrong format of e-gateway response template file
-4	No connection to the acquirer host (NS)
-5	The acquirer host (NS) connection failed during transaction processing
-6	e-Gateway configuration error
-7	The acquirer host (NS) response is invalid, e.g. mandatory fields missing
-8	Error in the "Card number" request field
-9	Error in the "Card expiration date" request field
-10	Error in the "Amount" request field
-11	Error in the "Currency" request field
-12	Error in the "Merchant ID" request field
-13	The referrer IP address (usually the merchant's IP) is not the one expected
-14	No connection to the iPOS PINpad or agent program is not running on the iPOS computer/workstation
-15	Error in the "RRN" request field
-16	Another transaction is being performed on the terminal
-17	The terminal is denied access to the e-Gateway
-18	Error in the CVC2 or CVC2 Description request fields
-19	Error in the authentication information request or authentication failed.
-20	A permitted time interval (1 hour by default) between the transaction Time Stamp request field and the e-Gateway time is exceeded
-21	The transaction has already been executed
-22	Transaction contains invalid authentication information
-23	Invalid transaction context
-24	Transaction context data mismatch
-25	Transaction canceled (e.g. by user)
-26	Invalid action BIN
-27	Invalid merchant name
-28	Invalid incoming addendum(s)
-29	Invalid/duplicate authentication reference
-30	Transaction was declined as fraud
-31	Transaction already in progress
-32	Duplicate declined transaction
-33	Client authentication by random amount or verify one-time code in progress
-34	MasterCard Installment client choice in progress
-35	MasterCard Installments auto canceled
-97	Session Timeout / Not Login
-98	Exceed OTP attempts limit
-99	Transaction aborted due to browser refresh