

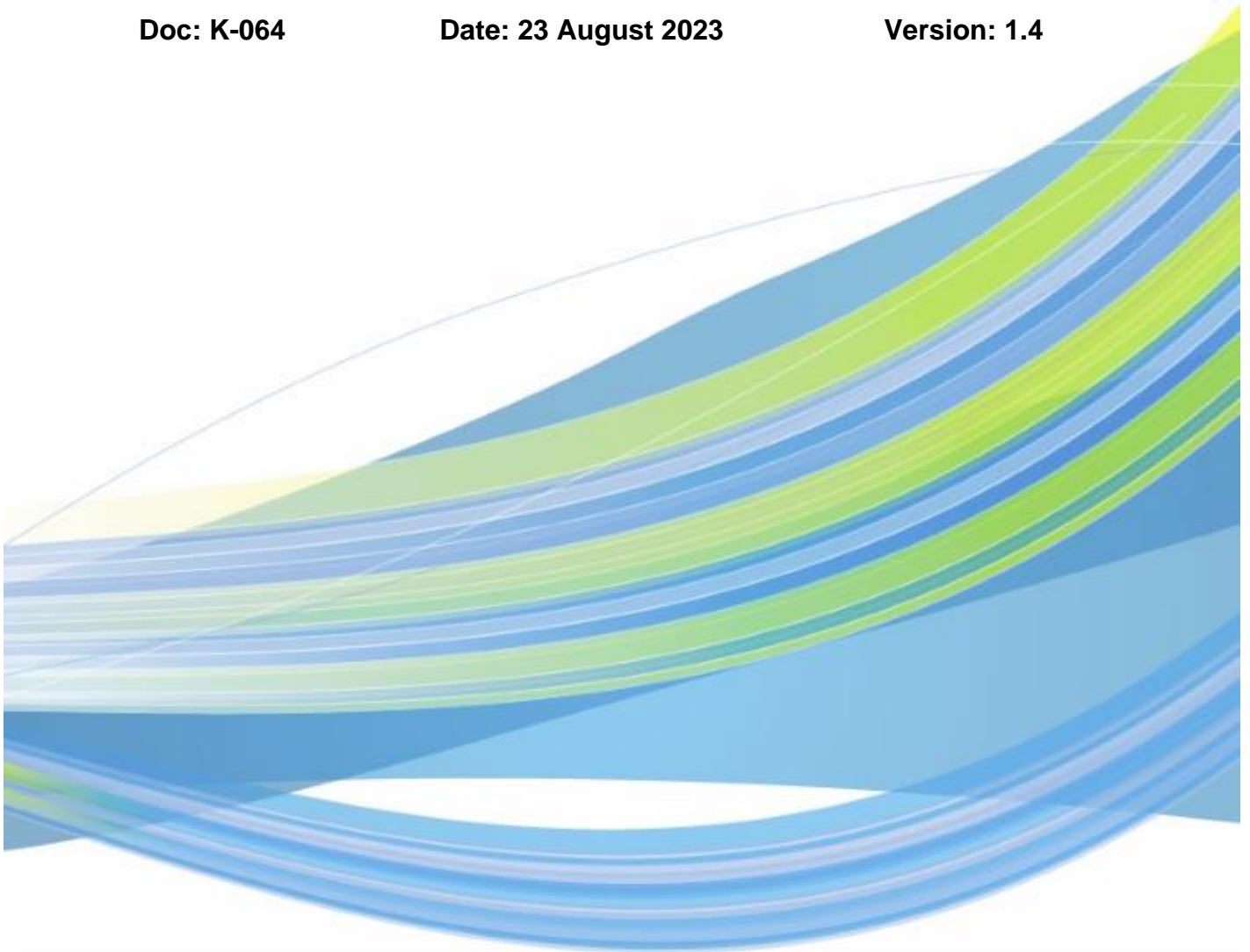


Merchant Integration Manual

Doc: K-064

Date: 23 August 2023

Version: 1.4



All rights reserved

This document or any part thereof may not be reproduced or used in any manner whatsoever without the express prior permission of KNET Management

Revision History

Version	Status	Updated By	Date	Summary of Updates
Draft	Initial Version	ADD	04 Mar 2019	Initial Draft
1.0	Updated Draft	ADD/QAD	01 Nov 2020	Updated Draft
1.1	Updated Version	ADD/QAD	01 Jan 2021	Document re-issue for new PG and new services added Version 1.1 – 2021 (Refund)
1.2	Updated Version	ADD/QAD	06 Feb 2022	Annual Review (2022)
1.3	Updated Version	ADD/QAD	27 Dec 2022	Addition of Section 8.1 (Certification of KFAST)
1.4	Updated Version	Application Engineering/ Quality Mgmt.	23 Aug 2023	<ul style="list-style-type: none"> - Section 2.3 – SSL/HTTPS Prerequisites <ul style="list-style-type: none"> o 'Note' changed to 'Notes' o Addition of point 2 under 'Notes'- <i>"The Merchant's SSL ... the KNET Payment Gateway Server."</i> - Section 3 – Merchant Integration Process <ul style="list-style-type: none"> o 3.1 – Integration Process : Note 1) – Removal of 'KNET will not verify whether the merchant has received a transaction response or not o Sub-section 3.4 and onwards renumbered to accommodate new sub-section 3.4 – SSL Certification Import o Addition of sub-section 3.5.2 – Transaction Response Notification; further sub-sections renumbered o Sub-section 3.5.3 - Note - Removal of 'KNET will not verify whether the merchant has received a transaction response or not. - Section 5 – Response Notification <ul style="list-style-type: none"> o New paragraphs (2 and 3) added – <i>"The merchant must</i>

				<p>then process...URL>"; and "Payment Gateway will then read.. payment initialization"</p> <ul style="list-style-type: none"> - Section 8 - Certification <ul style="list-style-type: none"> o Point 3 moved to Point 4 to accommodate new Point 3 – "Merchant must provide KNET with...knet.com.kw" o Subsequent points renumbered - Section 9 – Troubleshooting reference <ul style="list-style-type: none"> o 9.2.1 <ul style="list-style-type: none"> ▪ Heading changed from "Not receiving the Response Notification" to "Auto-void issue or notification response not reaching merchant server, namely responseURL" ▪ Point 2 rewritten ▪ Points 3 to 6 added - Section 12 – Best Practices <ul style="list-style-type: none"> o 12.1 – Removal of Point 'd' "Transaction response happens via customer redirections so it depends on customer's internet which could lead to missing response for a certain transactions, therefore it's MERCHANTS RESPONSIBILITY TO USE INQUIRY to check the status of such incomplete orders" o 12.2 – 'd' moved to "e" to accommodate new point 'd' – "The Merchant can use ...incomplete orders"
--	--	--	--	---



Contents

1.	Purpose	1
1.1.	Target Audience	1
2.	Merchant Prerequisites	2
2.1	Hardware Prerequisites	2
2.2	Software Prerequisites	2
2.3	SSL / HTTPS Prerequisites	3
3.	Merchant Integration Process	4
3.1	Integration Process.....	4
3.2	Download Plug-in	5
3.3	Downloading Resource and Key store Files	6
3.4	SSL Certificate Import	6
3.5	Transaction Processing	6
3.6	Integrate plug-in/resource file with merchant webpage	11
3.7	Refund API	15
4.	Transaction Testing	17
5.	Response Notification.....	18
6.	KFAST	20
7.	Refund	21
8.	Certification	29
8.1	Certification for KFAST	30
9.	Troubleshooting Reference	32
9.1	Errors in initialization or inquiry	32
9.2	Not Receiving the Response Notification	33
10.	Error Codes and Description:	34
11.	Sample Demo Page Navigation	48
12.	Best Practices	50
12.1	Mandatory	50
12.2	Recommended	50
13	Document Update Notice	52

1. Purpose

The purpose of this document is to provide supplementary technical information on merchant website integration with KNET Payment Gateway.

1.1. Target Audience

The target audiences for this document are:

- 1) Any developer/integrator working on behalf of / for any merchant who has signed up with KNET member banks to process transactions on KNET Payment Gateway.
- 2) Any administrator or acquirer institution user who requires appropriate information on the KNET Payment Gateway integration process.

Note: *It is imperative that 3rd parties/merchants have signed an NDA before sharing this document with them.*

2. Merchant Prerequisites

Readers of this user guide should be familiar with any of the JSP, ASP .Net, PHP or Java languages.

2.1 Hardware Prerequisites

2.1.1 Merchants can use their existing hardware for transaction processing via Payment Gateway provided

- I. They have a variety of arrangements for hosting their websites.
- II. Have relevant security mandates for internet access controls and checks. This may include utilization of a Proxy Server which presents informed challenges.

2.1.2 It is recommended that the merchant uses a Public IP during the integration testing for transaction processing to the Payment Gateway. The merchant should ensure the Payment Gateway Domain and IP address is enabled at the firewall for both incoming and outgoing request/response.

2.1.3 In order to send the authorization details to a merchant web server, the https port of the merchant web server should be made accessible to the KNET Payment Gateway Server.

Note: *KNET will ONLY accept https communication between the KNET Payment Gateway (Port: 443) and a merchant website since the information being exchanged is sensitive (password, terminal ID, etc.).*

2.2 Software Prerequisites

KNET supports the following types of software plug-ins:

- a) Java
- b) ASP.NET
- c) PHP
- d) RAW

The merchant should have the requisite software for connecting to the Payment Gateway depending on the merchant application environment, and may use combinations of OS/Web Server/Application server whilst setting up and operating the website.

Standard Software options are listed below: (this list is for reference use only)

- i. Operating Systems: Windows Server, Sun Solaris, IBM AIX Web/Application Servers - Web/Application Server that support JSP, PHP & ASP.NET. The current version with all required patches is recommended to ensure successful integration.
- ii. Software Installation – Basic software that are required for Web/Application server should be installed at the merchant site. (Java/JDK for JSP integration is essential; similarly, .NET frame work is essential for ASP.NET integration)

2.3 SSL / HTTPS Prerequisites

The merchant's web server should have a valid SSL certificate to receive the response from KNET. The KNET server will receive transactions only from HTTPS enabled web servers. It is the merchant's responsibility to contact an authorized certificate authority and purchase their own certificate.

Notes:

- *KNET will not provide an SSL certificate for the merchant.*
- *The Merchant's SSL certificate along with its intermediate and root certificates will be imported on to the KNET Payment Gateway Server.*

3. Merchant Integration Process

3.1 Integration Process

Steps to be followed by a Merchant Integration Team:

- 1) Login to the certification environment with the user credential shared by KNET using below URL <https://www.kpaytest.com.kw/kpg/merchant.htm> (test) OR <https://www.kpay.com.kw/portal/merchant.htm> (production).
- 2) Download the respective plug-in (based on the platform (Java/ASP.NET/PHP etc.) and method (Library or RAW) to connect Payment Gateway from the menu "Merchant Process -> Plug-in Download".
 - a. In case Library based method will be used to integrate PG, Merchant should download the Resource file & Keystore file from the menu "Merchant Process -> Resource File Download" and obtain the resource alias from the menu "Merchant Process -> View Terminal -> Plugin".
 - b. In case RAW based method will be used to integrate PG, Merchant should obtain the Tranportal ID from the menu "Merchant Process -> View Terminal -> Plugin" and request for the Tranportal Password and Terminal Resource Key from the Merchant Support Department.
- 3) Copy all files to a certain folder location e.g. /usr/local/paymentgateway/.
- 4) Integrate the plug-in with merchant web page using this document by constructing the request message as expected by Payment Gateway.
- 5) Process the response message received from Payment Gateway.

NOTES: Merchant Responsibilities

- 1) *It is the merchant's responsibility to use transaction inquiry to retrieve transaction details.*
- 2) *It is the merchant's responsibility to keep the configuration files & terminal details / key secure to prevent data forging or possible fraud.*



3.2 Download Plug-in

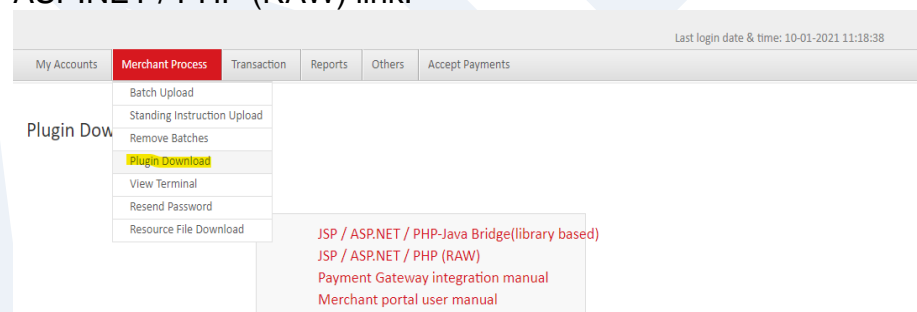
3.2.1 JSP / ASP.NET / PHP-Java Bridge (library based) Plug-in

To download the JSP / ASP.NET / PHP-Java Bridge (library based) Plug-in, click JSP / ASP.NET / PHP-Java Bridge (library based) link.

- a) For JAVA plugin, use the **java** folder from the extracted RAR file.
 - I. Copy all the jar files and paste it in merchant application lib folder.
 - II. Copy bcprov-jdk15-145.jar from extracted RAR file and paste it in Java\jdk1.6.0_26\jre\lib\ext.
 - III. Add the below entry in the java.security file (Java\jdk1.6.0_26\jre\lib\security)
security.provider.10=org.bouncycastle.jce.provider.BouncyCastleProvider
- b) For ASP.NET plugin use **asp.net** folder from the extracted RAR file
 - i. Ipaypipe.dll and other supporting DLL files can be copied from the folder.

3.2.2 JSP / ASP.NET / PHP (RAW)

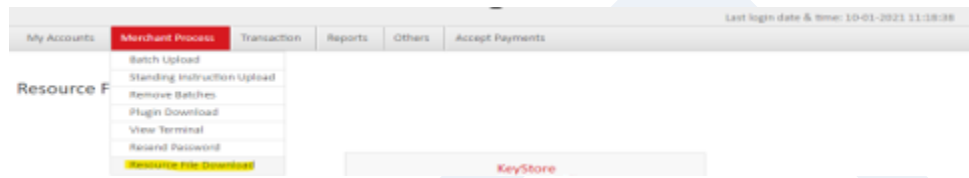
To download the JSP / ASP.NET / PHP Raw interface KIT, click on JSP / ASP.NET / PHP (RAW) link.



3.3 Downloading Resource and Key store Files

Click on Merchant Process > Resource File Download

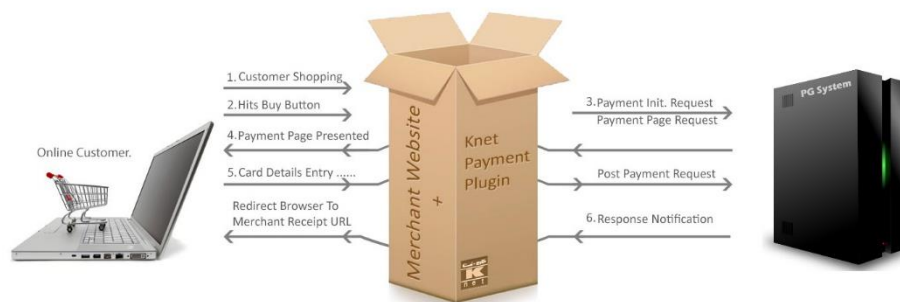
Move the downloaded resource & Key store files to a specific folder e.g.
C:\resourcepath



3.4 SSL Certificate Import

Merchant must provide a copy of the website's SSL certificate for KNET to import it into the Payment Gateway environment.

3.5 Transaction Processing



3.5.1 Standard Payment Flow

1. Customer is shopping on the merchant site.
2. Customer completes shopping; proceeds to check out.
3. Merchant gathers required information from customer, including the total customer bill amount.
4. Merchant performs payment initialization with KNET PG on the required

amount.

5. On successful payment initialization, KNET PG replies with the KNET payment URL.
6. Merchant saves payment initialization parameters with track ID being the primary key, and redirects the customer to the KNET payment page.
7. KNET builds the payment page and sends it to the customer.
8. Customer enters card information and clicks 'Submit'
9. KNET processes the transaction. If no error occurs, KNET sends the transaction response to the Merchant Response URL specified in payment initialization.
10. Merchant can send an inquiry transaction to KNET to verify the transaction status before giving the service / product.

NOTE: It is the merchant's responsibility to use transaction inquiry to retrieve transaction details.

3.5.2 Transaction Response Notification

If payment is initialized and the customer is redirected to KNET payment page, the customer enters his/her card details on the KNET payment page. After the customer submits card information, KNET will process the request and send back the response as a URL Encoded POST request to the notification URL specified by the merchant in the payment initialization request, namely responseURL. The Merchant MUST save the returned values by KNET in their database.

3.5.3 Transaction Inquiry

KNET allows merchants to do an inquiry on transactions by passing the transaction details to Payment Gateway. Payment Gateway will then respond with the transaction response details. It is the merchant's responsibility to verify that the details received back from inquiry tally with their records, or in case response notification has not been received at the merchant's end. Transaction inquiry is initiated from merchant to KNET using a server to server call. Refer to the integration section in the document for snippet code samples to integrate inquiry.

Important Notes:

- An inquiry can be sent using multiple identifiers to identify the original transaction; transaction id, payment id, track id, reference id.
- The udf5 parameter should include the parameter tag that will be used to identify the original transaction e.g. "TrackID" or "PaymentID" or

“TransactionID” or “RefID”. If *udf5* is sent empty then Payment Gateway will set the inquiry identifier by default to “TransactionID”.

- The transid parameter should include the parameter value of the original transaction which is defined in *udf5*.
- The amount parameter has to be included in the inquiry request and should hold the amount value of the original transaction.
- The track ID parameter has to be included in the inquiry request and should hold the track ID value of the original transaction.

Refer to the table below for more details

Inquire by	transid	Udf5	amt	trackid
Transaction ID	Original TransId	Empty or TransId	Original Amount	Original TrackId
Track ID	Original TrackId	TrackID	Original Amount	Original TrackId
Payment ID	Original PaymentId	PaymentID	Original Amount	Original TrackId
Reference ID	Original RefId	RefID	Original Amount	Original TrackId

NOTE: It is the merchant’s responsibility to use transaction inquiry to retrieve transaction details.

3.5.4 Payment Trans. Initialization Transmit Msg Variables and Definitions

Variable	Type	Length	Required	Description
Resource Path	STRING	255	Y (Library based Integration)	Resource Path is the absolute path to the folder which contains the resource file
Key store Path	STRING	255	Y ((Library based Integration)	Keystore Path is the absolute path to the folder which contains the key store file
Tran Portal ID	STRING	255	Y (RAW based Integration)	Unique ID assigned for each terminal. You can extract the Tran Portal ID from the portal (Merchant Process > View Terminal > Plugin)
Tran portal password	STRING	15	Y (RAW based Integration)	Password assigned for a terminal. Please contact acquirer bank / KNET to extract the terminal password
Terminal Resource Key	STRING	16	Y (RAW based Integration)	Terminal key for encrypting / decrypting the communication with Payment Gateway. Please contact acquirer bank / KNET to extract the terminal password
Alias	STRING	25	Y(Library based Integration)	Alias name is required for the plugin read the contents of the resource file. You can extract the alias from the portal (Merchant Process > View Terminal > Plugin)

Action	STRING	1	Y	Value must always be in numeric format (1 for Purchase transactions, 8 for inquiry)
Amount	STRING	10	Y	Transaction amount should be passed as STRING. The amount value should include the decimal point (always 3 for Kuwaiti Dinars), e.g. 15.750, 10.000 etc. In inquiry, amount should be set to the amount of the original transaction
Currency Code	STRING	3	Y	The currency code of the transaction. For KD, use currency code 414
Language	STRING	3	Y	The language of the KNET payment page when presented to the customer. For English, use the string "EN" For Arabic, use the string "AR"
Response URL	STRING	255	Y	The URL which Payment Gateway will attempt to send the transaction response details
Error URL	STRING	255	Y	The URL to redirect the consumer browser to, if an error occurs
Track ID	STRING	40	Y	A unique tracking id generated by the merchant's commerce system which is stored with the transaction (avoid spaces and extended characters, only alpha-numeric is to be used). The merchant should initiate such ID to be unique for every transaction initialized irrespective of the customer. The merchant should store the track id in their database for their records. In inquiry, track id should be set to the track id of the original transaction
Trans ID	STRING	19	Y (Refund / Inquiry)	Used to identify the original transaction for an inquiry transaction. The value assigned could be Transaction ID, Track ID, Reference ID or Payment ID depending on the UDF5 value assigned
UDF1-4	STRING	255	N	User Defined Fields 1,2,3,4 can be used to pass and store any additional transaction data required to be archived with the transaction and available as a searching criteria
UDF3 (KFast)	STRING	8	N	In order to user the KFAST services merchant should pass 8 digit numeric value as customer identifier. e.g. UDF3="12345678" Once user has registered his card at payment page, for all his future transactions his registered card(s) will be shown on the payment page as long as merchant is sending the same ID for this customer.
UDF5	STRING	255	N	User Defined Field 5, can be used to pass and store any additional transaction data required to be archived with the transaction and available as a

				<p>searching criteria.</p> <p>Purchase: This field has been dedicated for merchants who would like to pass additional customer data and wish to include it in the acquiring bank's report. Merchants can use UDF5 to pass the additional data preceded by the text "ptlf" as follows: UDF5 = "ptlf amx1234567890". For example, if the additional customer data is amx1234567890 and merchant would like to see this value in the acquiring bank report, then UDF5 should be in the following format: UDF5 = "ptlf amx1234567890"</p> <p>Note: Merchants must not exceed 50 characters including ptlf when using ptlf in UDF5</p> <p>Inquiry: Inquiry is initiated based on the value assigned here. For example, if inquiry is to be on merchant track ID basis then UDF5 should be set to the following: UDF5 = "TrackID"</p> <p>By default, it is on Transaction ID basis unless value is assigned otherwise</p>
--	--	--	--	--

3.5.5 Payment Transaction Response Message Variables and Definitions

Variable	Description
Payment ID	Unique order ID generated by Payment Gateway. Merchant must map this value in their records to the corresponding track ID and transaction ID.
Result	<p>Returned as the transaction response evaluator. The Result should be evaluated to determine if the transaction has been performed successfully after checking for errors. The merchant should first check for any error received; if no error received, check for the result parameter value corresponding to the below:</p> <ul style="list-style-type: none"> • CAPTURED - Transaction was approved • NOT CAPTURED - Transaction was not approved • CANCELED – Transaction was canceled by customer on the payment page • HOST TIMEOUT - The authorization system did not respond within the timeout limit <p>The below results are returned in case of inquiry:</p> <ul style="list-style-type: none"> • SUCCESS or CAPTURED - Transaction is available and payment was captured successfully • FAILURE or SUSPECTED or errors - Transaction has failed
Reference ID	The unique resulting reference number of the transaction generated by KNET. This number or series of letters is used for referential purposes by some acquiring institutions and should be stored properly.
Track ID	The Track ID is generated by the merchant in the transaction request



Transaction ID	Unique ID generated by Payment Gateway for the transaction
Post Date	Transaction Post Date in the format of "MMDD". Postdate is used for reconciliation purpose and it can be different than the actual date in some cases.
Auth	The resulting authorization number of the transaction generated by the bank
UDF1-UDF5	User Defined Fields 1-5 can be used to pass and store any additional transaction data required to be archived with the transaction and available as a searching criteria
Amount	Transaction Amount in three decimal form
avr	Address verification response
authRespCode	This is the response code i.e. the reason code for the transaction. Merchant can use this code for additional validation of the transaction and can also use this response code field along with the reason code description list.
Error Text	Error description in case transaction is not successful
Error	Error code in case transaction is not successful

3.6 Integrate plug-in/resource file with merchant webpage

3.6.1. Code snippet for JSP Integration

a. KNET Hosted Payment Integration (Purchase)

```
iPayPipe pipe = new iPayPipe();

String resourcePath = "c:\\resourcepath";
String keystorePath = "c:\\keystorePath";
String receiptURL= "http://www.demomerchant.com/result.jsp";
String errorURL= "http://www.demomerchant.com/error.jsp";
String action="1";
String alias = "alias";
String currency = "414";
String language = "language"; // English - "EN", Arabic - "AR"
String amount = "1000.000";
String trackid = "109088888";
String Udf1= "Udf1";
String Udf2= "Udf2";
String Udf3= "Udf3";
String Udf4= "Udf4";
String Udf5= "Udf5";

pipe.setResourcePath(resourcePath);
pipe.setKeystorePath(keystorePath);
pipe.setAlias(alias);
pipe.setAction(action);
pipe.setCurrency(currency);
```



```
pipe.setLanguage(language);  
pipe.setResponseURL( receiptURL );  
pipe.setErrorURL(errorURL);  
pipe.setAmt(amount);  
pipe.setTrackId(trackid);  
pipe.setUdf1(Udf1);  
pipe.setUdf2(Udf2);  
pipe.setUdf3(Udf3);  
pipe.setUdf4(Udf4);  
pipe.setUdf5(Udf5);
```

```
int val = pipe.performPaymentInitializationHTTP();
```

```
if(val==0){  
    response.sendRedirect(pipe.getWebAddress());  
}else{  
    pipe.getError();  
}
```

Once the cardholder has been redirected to the KNET payment page and fills in the required details, Payment Gateway will send the transaction response details to the merchant response URL in the below encrypted form.

```
trandata=1C1A967D16C877543E0A1DD90D2933853F05BB0AA2E6B47BB77D27EEAF32EF02CF6A0A5643  
F31C78340913929D90879615DFA9CDCCBB03761B9AE87CD76FE8633E0A1DD90D29338545DA582B0F3500BA93  
75313637690  
531C6D7F8F7489C7CD8B73F9EC7E1C622DDD06B0809A709C2CB2A6EFD72F36FEB044B73810204E69FC577300  
F9A  
AF38E044F0A34694348506778257040533E4FD48A9C61DD83E906AB93110CE0E57A1C548FA589B8F856  
6FC9F
```

To decrypt the above response, merchant should follow the steps below:

```
iPayPipe pipe = new iPayPipe();
```

```
String resourcePath = "c:\\resourcepath";  
String keystorePath = "c:\\keystorePath";  
String aliasName = "alias";
```

```
pipe.setResourcePath(resourcePath);  
pipe.setKeystorePath(keystorePath);  
pipe.setAlias(aliasName);
```

```
String errorText = request.getParameter("ErrorText");
```

```
int result = pipe.parseEncryptedRequest(request.getParameter("trandata"));
```

```
if(result!=0){  
    pipe.getError();  
}else{  
    if(errorText==null){  
        pipe.getResult();  
        pipe.getDate();  
        pipe.getRef();  
    }
```



```
        pipe.getTrackId();
        pipe.getTransId();
        pipe.getAmt();
        pipe.getUdf1();
        pipe.getUdf2();
        pipe.getUdf3();
        pipe.getUdf4();
        pipe.getUdf5();
        pipe.getPaymentId();
    }else
    {
        request.getParameter("ErrorText");
        request.getParameter("paymentid");
        request.getParameter("Error");
        request.getParameter("trackid");
        request.getParameter("amt");
        request.getParameter("trackid");
        request.getParameter("udf1");
        request.getParameter("udf2");
        request.getParameter("udf3");
        request.getParameter("udf4");
        request.getParameter("udf5");
    }
}
```

b. KNET Tranportal Payment Integration (Inquiry)

```
iPayPipe pipe = new iPayPipe();

String resourcePath = "c:\\resourcepath";
String keystorePath = "c:\\keystorePath";
String action="8";
String alias = "alias";
String trackid = "109088888";
String currency = "414";
String amount = "1000.000";
String Udf1= "Udf1";
String Udf2= "Udf2";
String Udf3= "Udf3";
String Udf4= "Udf4";
String Udf5= "TransID";
String transId = "201905876947223";
```

NOTE: A merchant can initiate inquiry transaction using :

- PG Transaction ID – *[in UDF5 field “**TransID**” and in transId field PG transaction ID to be sent].*
- PG Payment ID – *[in UDF5 field “**PaymentID**” and in transId field PG Payment ID to be sent].*
- Merchant Track ID – *[in UDF5 field “**TrackID**” and in transId field MerchantTrack ID to be sent].*
(If inquiry initiated with TrackID, then the trackID passed in the transID field and the trackID passed in the inquiry request need to be the same)
- PG Reference ID – *[in UDF5 field “**SeqNum**” and in transID field reference number to be sent].*

```
pipe.setResourcePath(resourcePath);
pipe.setKeystorePath(keystorePath);
pipe.setAlias(alias);
pipe.setAction(action);
pipe.setCurrency(currency);
pipe.setAmt(amount);
pipe.setTransId(transId);
pipe.setTrackId(trackid);
pipe.setUdf1(Udf1);
pipe.setUdf2(Udf2);
pipe.setUdf3(Udf3);
pipe.setUdf4(Udf4);
pipe.setUdf5(Udf5);

int val = pipe.performTransaction();

if(val==0){
    pipe.getResult();
    pipe.getPaymentId();
    pipe.getTransId();
    pipe.getAmt();
}else
{
    pipe.getError();
}
```

3.6.2 ASP.NET Integration

- a) KNET HOSTED Payment Integration (PURCHASE)
- b) KNET Tranportal Payment Integration (INQUIRY)

Registering ASP. NET Plug-in the Merchant Server

- Make sure to place the provided DLLs into a certain physical path on the system.
- Add reference to the DLLs into your application by following the below steps:
 - Right Click the **Reference** tab of the Solution Explorer in the Visual studio IDE and click 'Add Reference'
 - In the **Add Reference** Dialog box, browse the DLL's Physical path and click 'Ok'
 - Once the process is done correctly all the DLLs will be visible (referred & supported) into the BIN folder of the Application.
 - In order to use the iPayPipe in the application, add the java package into the .NET application by adding the "**using com.fss.plugin;**" namespace in the corresponding ASP pages.

3.7 Refund API

The API refund feature is real time therefore it is merchant responsibility to test the feature properly and ensure it is integrated properly. Merchant has to ensure that only authorized personnel's have access to this feature to avoid financial loss. KNET will not be held responsible for any loss or misuse because this feature has not yet been certified or released by KNET.

3.7.1 API Method

If you will be using the Library based method to refund:

```
Library based request Sample (refund) :
iPayPipe pipe = new iPayPipe();
pipe.setResourcePath("Full Absolute Path to Your Resource File");
pipe.setKeystorePath("Full Absolute Path to Your Keystore File");
pipe.setAlias("Alias here");
pipe.setCurrency("414");
pipe.setAction("2");
pipe.setAmt("2.000");

// If you will refund based on the track ID then you will have to set: // The track ID
value of the original transaction in the transid parameter & trackid parameter // UDF5 to
"TrackID" similar to the above sample.
pipe.setUdf5("TrackID");
pipe.setTransId("Track ID Value");
pipe.setTrackId("Track ID Value");
```



```
if (pipe.performTransaction() == 0) { // Merchant should consider the refund as success
only if result parameter returns CAPTURED otherwise any other value should be considered
failure. pipe.getResult(); } else { // Merchant to handle the error scenario similar
to purchase transactions as mentioned in the PG integration document }
```

3.7.2 RAW Method

If you will be using the RAW based method to refund:

URL to Connect: Test: <https://www.kpaytest.com.kw/kpg/tranPipe.htm?param=tranInit&>

Production: <https://www.kpay.com.kw/kpg/tranPipe.htm?param=tranInit&>

Headers: Content-type: application/xml

RAW based request Sample (refund) :

```
<id>Terminal ID</id>
<password>Terminal Password</password>
<action>2</action>
<amt>2.000</amt>
<transid>Track ID Value</transid>
<trackid>Track ID Value</trackid>
<udf5>TrackID</udf5>
```

// If you will refund based on the track ID then you will have to set: // The track ID value of the original transaction in the transid parameter & trackid parameter // UDF5 to "TrackID" similar to the above sample. .

3.7.3 Response parameters and datatype

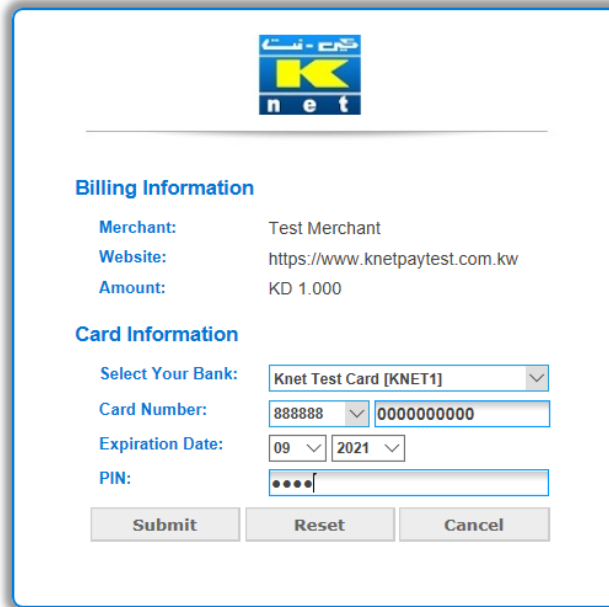
Field Name	Data Type
Result	String()

Merchant should consider the refund as success only if result parameter returns CAPTURED otherwise any other value should be considered failure.

Example HTTP response:

```
<result>CAPTURED</result><payid>100201719515482162</payid><trackid>
6078874794527794643</trackid><udf1>
</udf1><udf5></udf5><ref></ref><auth></auth><postdate></postdate><tranid></tranid><amt></amt>
```

4. Transaction Testing



The image shows a web form for KNET Test Card [KNET1]. The form is titled "Billing Information" and "Card Information". It contains fields for Merchant, Website, Amount, Card Number, Expiration Date, and PIN. The form is displayed in a window with the KNET logo at the top.

Billing Information	
Merchant:	Test Merchant
Website:	https://www.knetpaytest.com.kw
Amount:	KD 1.000

Card Information	
Select Your Bank:	Knet Test Card [KNET1]
Card Number:	888888 0000000000
Expiration Date:	09/2021
PIN:

Submit Reset Cancel

Merchants can use **KNET Test Card [KNET1]** to complete transactions in the test environment, listed in the dropdown bank list on the payment page. To simulate the CAPTURED (transaction is approved by bank) result value, merchant has to set the Expiration Date to **09/2021**. Expiration Date other than the above mentioned will result in NOT CAPTURED (transaction is declined by the bank).

Note: PIN can be set to any numeric 4 digit value in test environment.

5. Response Notification

If payment is initialized and the customer is redirected to KNET payment page, the customer enters his/her card details on the KNET payment page. After the customer submits card information, KNET will process the request and send back the encrypted response as a URL Encoded POST request to the notification URL specified by the merchant in the payment initialization request, namely responseURL. The Merchant MUST decrypt the response and cross verify the returned values with their database. The Merchant MUST save both encrypted & plain text response details in their database.

The merchant must then process the response and store the transaction response detail; after which the Merchant Notification URL must write a single line response to the Payment Gateway in the following form:

REDIRECT=<Merchant Receipt URL>

Payment Gateway will then read the response from the Merchant Notification URL page and redirect the customer to the Merchant Receipt Page where the merchant will present the customer with the transaction response details. If for any reason KNET Payment Gateway cannot process the customer transaction, KNET will redirect the customer to the merchant error URL specified in errorURL parameter sent in payment initialization.

Merchants can use the inquiry feature to verify the transaction details or in case the response did not reach the merchant due to customer having closed the browser before redirecting back to merchant website, network fluctuations, etc.

Transaction Response Sample:

The plain text response message is formatted differently according to the result value:

CAPTURED: Transaction is approved by the bank

```
paymentid=8962225231041180&result=CAPTURED&auth=999554  
&avr=N&ref=411857974849&tranid=9929892231041180&postdate=0427&tracki  
d=632186&udf1=&udf2=&udf3=&udf4=&udf5=&amt=20.550&authResponseCod  
e=00
```

NOT CAPTURED: Transaction is declined by the bank

```
paymentid=8962225231041180&result=NOT+CAPTURED&auth=999554  
&avr=N&ref=411857974849&tranid=9929892231041180&postdate=0427&tracki  
d=632186&udf1=&udf2=&udf3=&udf4=&udf5=&amt=20.550&authResponseCod  
e=00
```

HOST TIMEOUT: Bank does not respond within the timeout period

```
paymentid=8962225231041180&result=HOST+TIMEOUT&auth=999554
```



Title : **Merchant Integration Manual**

Version : 1.4

Doc : K-064

Date : 23 Aug. 2023

Section : Response Notification

Section : 5

&avr=N&ref=411857974849&tranid=9929892231041180&postdate=0427&trackid=632186&udf1=&udf2=&udf3=&udf4=&udf5=&amt=20.550

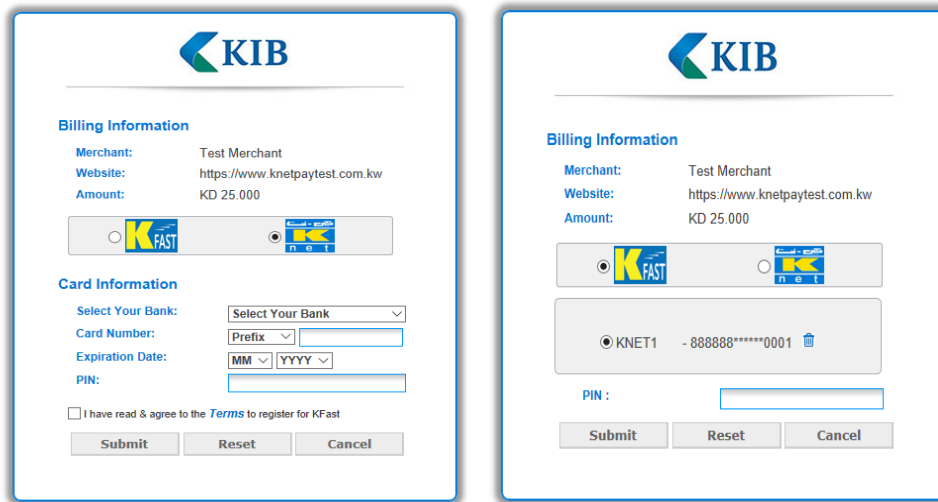
CANCELED: Customer canceled the transaction.

paymentid=8962225231041180&result=CANCELED&auth=&avr=N
&ref=&tranid=&postdate=&trackid=632186&udf1=&udf2=&udf3=&udf4=&udf5=&amt=20.550

6. KFAST

KFAST is a feature offered by Payment Gateway to facilitate a faster checkout experience for customers. Once registered, the cardholder is no longer required to enter the card number and expiry date, only the PIN will be required. To opt for this feature, a merchant has to contact their acquirer bank and request the service.

Merchants can navigate through the merchant portal to **Merchant Process > View Terminal** to check whether KFAST is enabled on the terminal profile.



The image shows two screenshots of the KIB merchant portal. The left screenshot displays the 'Billing Information' section with fields for Merchant (Test Merchant), Website (https://www.knetpaytest.com.kw), and Amount (KD 25.000). Below this is a radio button selection for KFAST, which is currently unselected. The 'Card Information' section includes a 'Select Your Bank' dropdown, 'Card Number' (Prefix and main number), 'Expiration Date' (MM and YYYY), and 'PIN'. A checkbox for 'I have read & agree to the Terms to register for KFast' is also present. The right screenshot shows the same 'Billing Information' section, but the KFAST radio button is now selected. Below it, a numeric token is displayed: KNET1 - 888888*****0001. A PIN field is also visible.

To enable KFAST on the payment page, the merchant has to pass a numeric token of 8 digits in UDF3 parameter in the following format:

To enable KFAST feature on the KNET Payment page	Parameter	Type	Token Length	Example
	UDF3	Numeric	8	pipe.setUdf3("17653474") or UDF3="17653474" (RAW)

KFAST option will be available once a customer has registered at least a single card by completing the payment & agreeing to the terms. Ideally, OTP is required to register a card, therefore in the test environment, OTP delivery will be assigned to the merchant phone number. (Testing session can be scheduled by contacting the Payment Gateway Support Department).

Note: It is the merchant's responsibility to pass the correct token for each customer to avoid other customers seeing the card details.

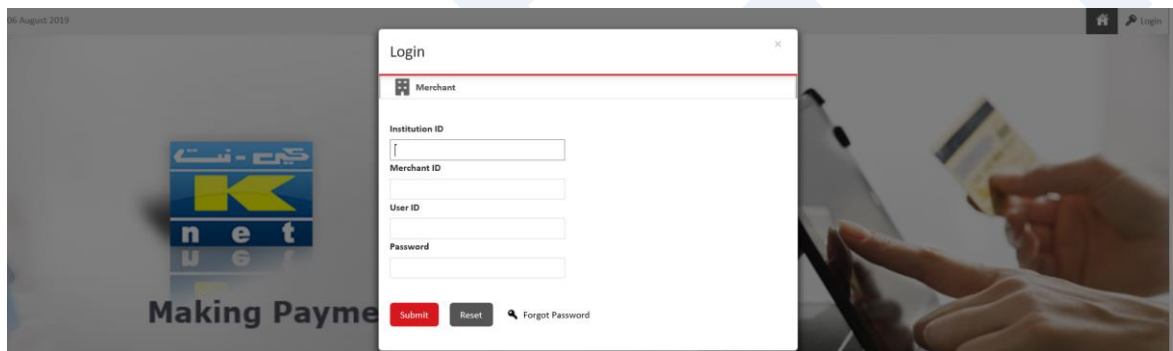
7. Refund

This section provides supplementary information to the subject who is authorized to generate refund transactions. This will serve as a guide to the end user who wants to make use of Payment Gateway's refund feature in cases whereby a merchant considers a transaction to be a dispute or some such other case. Payment Gateway supports manual refund and batch refund (bulk) in full & partial amounts.

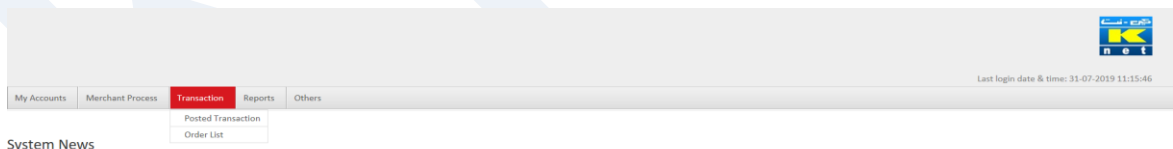
• Posted Transactions

The following screens demonstrate the steps to be carried out in refunding a transaction through Posted Transactions:

1. Login to the merchant site via the URL <https://www.kpay.com.kw/portal/merchant.htm> using the information provided to the merchant by KNET such as the institution id, merchant id, user id and password.



2. Navigate to **Transaction > Posted Transaction** to get the posted transactions management filter screen as shown below. Fill out the criteria fields if required. By default, the current date is set as both start and end dates. When done, click 'Search' to display the report.





Title : Merchant Integration Manual

Version : 1.4

Doc : K-064

Date : 23 Aug. 2023

Section : Refund

Section : 7

Search Merchant

Terminal ID*

ALL

Merchant Track ID

Authorization Code

Transaction Amount

(NNNNN.NNN)

Currency Code

ALL

Brand

ALL

Action

ALL

Search Date

Start Date*

06-08-2019 00:00:00

End Date*

06-08-2019 23:59:59

Sort By*

Transaction Date/Time

Search

3. The screen below is the posted transactions management report generated by the previous step. All transactions that meet the criteria as per the filled filter fields are displayed.

- Select the transaction to refund and select 'Credit' under the Action tab. By selecting the transaction, the amount of this transaction will appear in the text box (as shown below).
- Clicking on the Process button will refund the selected transactions.

Select	Action	Transaction Amount	Merchant ID	Terminal ID	Card Number	Transaction Date/Time	Transaction Action	Currency Code	Original Txn Amount	Merchant Track ID	Transaction ID	Reference ID
<input checked="" type="checkbox"/>	Credit	25.000	301	3010001	888888*****8883	August 6, 2019 11:01:24 AM AST	1-Purchase	414	25.000	5380181809545979549	201921839242387	921810000270
<input type="checkbox"/>	- Select -	25.000	301	3010001	888888*****8883	August 6, 2019 10:44:58 AM AST	1-Purchase	414	25.000	2114579770788514289	201921838749080	921810000250
<input type="checkbox"/>	Credit	25.777	301	3010001	888888*****8883	August 6, 2019 10:27:15 AM AST	1-Purchase	414	25.777	6521242037688861014	201921861782098	921810000214
<input type="checkbox"/>	- Select -	25.100	301	3010001	888888*****8883	August 6, 2019 10:22:47 AM AST	1-Purchase	414	25.100	8095225329223341584	201921838083816	921810000206
<input type="checkbox"/>	- Select -	24.999	301	3010001	888888*****8883	August 6, 2019 10:17:28 AM AST	1-Purchase	414	24.999	4118356374316809387	201921837924117	921810000195
<input type="checkbox"/>	- Select -	24.999	301	3010001	888888*****8883	August 6, 2019 10:15:39 AM AST	1-Purchase	414	24.999	3128107739188437781	201921862130019	921810000188
<input type="checkbox"/>	- Select -	1.000	301	3010001	888888*****8883	August 6, 2019 09:09:33 AM AST	1-Purchase	414	1.000	4509179576929393564	201921835886985	921810000099
<input type="checkbox"/>	- Select -	1.000	301	3010001	888888*****8883	August 6, 2019 09:06:34 AM AST	1-Purchase	414	1.000	8075414146624672891	201921864202703	921810000096
<input type="checkbox"/>	- Select -	25.000	301	3010001	888888*****8882	August 6, 2019 09:04:20 AM AST	1-Purchase	414	25.000	7926589248294397279	201921835730324	921810000095
<input type="checkbox"/>	- Select -	25.000	301	3010001	888888*****8882	August 6, 2019 09:03:26 AM AST	1-Purchase	414	25.000	8027851490521397496	201921835703204	921810000094

Next Last Process Back

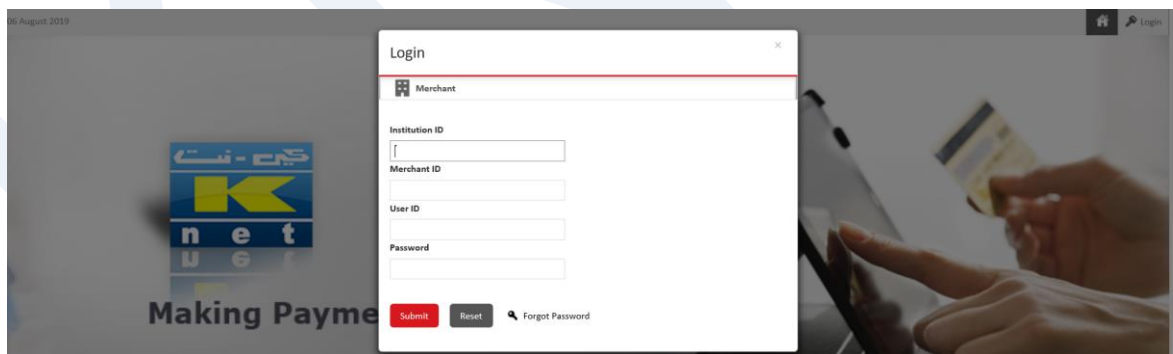
Note: The refund is considered successful only if the result code is CAPTURED.

Original Transaction ID	201921839242387	Batch ID	
IP Address	168.187.173.14	Post Date	0806
Transaction Date/Time	Tue Aug 06 11:28:51 AST 2019	Action Code	Credit
Transaction ID	201921859934168	Terminal ID	3010001
Merchant ID	301	Brand ID	Knet Test Card
Payment Instrument	Debit Card	Card Expiration	Aug , 2021
Card Number	888888*****8883	Currency Code	414
Transaction Amount	25.000	Result Code	CAPTURED
Merchant Track ID	5380181809545979549	Authorization Code	837927
Host Response	00	CVD2 Validation Repsonse	
AVS Response		STAN ID	571418
Reference ID	921810000298		
Cardholder Address		Cardholder Zip Code	
ECI	7	User Field 2	
User Field 1		User Field 4	
User Field 3			
User Field 5			
UCAF		Host Tran ID	

• Order List

The following screens demonstrate the steps to be carried out in refunding a transaction through Order List:

1. Login to the merchant site via the URL:
<https://www.kpay.com.kw/portal/merchant.htm> using the information provided to the merchant by KNET, i.e. institution id, merchant id, user id and password.



2. Navigate to **Transaction > Order List** to get the order list management filter screen as shown below. Fill out the criteria fields if required. By default, the current date is set as both start and end dates. When done, click 'Search' to display the report.

Search Merchant

Terminal ID*

ALL

Order Status*

ALL

Currency Code

ALL

Order ID

Merchant Track ID

Search Date

Start Date*

07-08-2019 00:00:00

End Date*

07-08-2019 23:59:59

Sort By*

Order Initialization Date/Time

Search

3. The screen shot below is the order list management report generated by the previous step. All transactions that meet the criteria as per filled filter fields are displayed.

- Click on the **Order ID** you wish to refund.
- Select the transaction to refund. By selecting the transaction, the amount of this transaction will appear in the text box (as shown below).
- Clicking on the **Credit** button will refund the selected transactions.

Order ID	Order Initialization Date/Time	Merchant ID	Terminal ID	Order Status	Currency Code	Merchant Track ID	Order Notify
100201921930640785	07-08-2019 10:01:21	301	3010001	PRESENTED	414	8433551300767734194	Y
100201921930619368	07-08-2019 10:00:38	301	3010001	PROCESSED	414	862796825080065058	Y

Select

Payment ID

Merchant ID

Terminal ID

CardNo

Action

Currency Code

Transaction Amount

Result Code

<input checked="" type="radio"/>	100201921930619368	301	3010001	888888*****0001	1-Purchase	414 - Kuwaiti Dinar	1.000	CAPTURED
----------------------------------	--------------------	-----	---------	-----------------	------------	---------------------	-------	----------

One item found.1

Credit

Capture

Detail

Back

1.000

Note: The refund is considered successful only if the result code is CAPTURED.

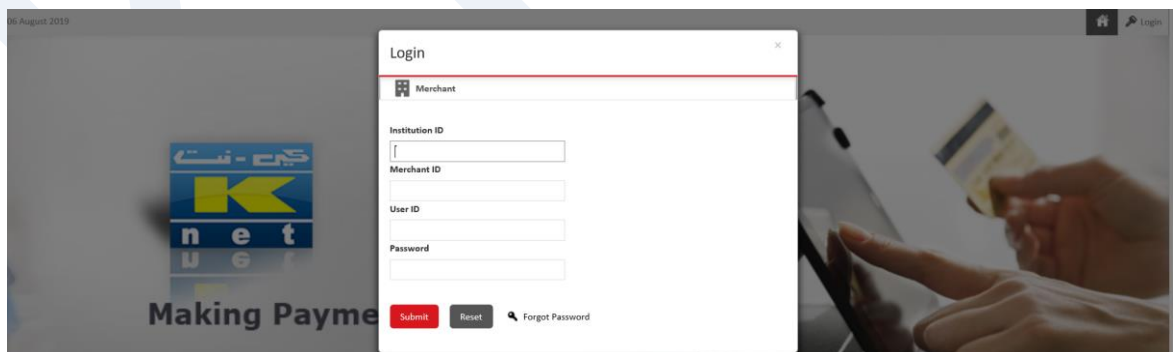
Original Transaction ID	201921930625831	Batch ID	
IP Address	10.249.0.78	Post Date	0807
Transaction Date/Time	Wed Aug 07 10:48:30 AST 2019	Action Code	Credit
Transaction ID	201921967944831	Terminal ID	3010001
Merchant ID	301	Brand ID	201825717889145
Payment Instrument	Debit Card	Card Expiration	Aug , 2021
Card Number	888888*****0001	Currency Code	414
Transaction Amount	1.000	Result Code	CAPTURED
Merchant Track ID	86279682508006508	Authorization Code	B05791
Host Response	00	CVD2 Validation Repsonse	
AVS Response		STAN ID	7336
Reference ID	921910000132		
Cardholder Address		Cardholder Zip Code	
ECI	7	User Field 2	
User Field 1		User Field 4	
User Field 3			
User Field 5			
UCAF		Host Tran ID	

• Batch Refund

To opt for this feature, the merchant has to contact their acquirer bank and request the service.

The following screen shots demonstrate the steps to be carried out in refunding a transaction through Order List:

1. Login to the merchant site via the URL <https://www.kpay.com.kw/portal/merchant.htm> using the information provided to the merchant by KNET, i.e. institution id, merchant id, user id and password.



2. Navigate to **Merchant Process > Batch Upload** to upload refunds in bulk. The batch file should be uploaded as a text file in the format shown below in a line separated format.

Batch Upload Sample Format

Header

Action Code,Card Number,Card Expire Date,CVV Number,Currency Code,Transaction id,ZIP,Address(Optional), Member Detail, Amount,Track Id, UDF1,UDF2,UDF3,UDF4,UDF5

Record

1,5453010000078071,1312,231,356, 5176358010014040,600000,Address, gopinath,150,12345675456, udf1,udf2,udf3,udf4,udf5

Cancel

batch2.txt - Notepad

File Edit Format View Help

2,,,414,201900635859030,,,0.500,3437,,,,,
2,,,414,201900635859030,,,0.500,3438,,,,,
2,,,414,201900635859030,,,0.500,3439,,,,,

Batch Upload Parameters:

Parameter	Type	Necessa ry	Value
Action Code	Numeric	Yes	2
Card Number	Numeric	No	Should be kept empty
Card Expire Date	Numeric	No	Should be kept empty
CVV Number	Numeric	No	Should be kept empty
Currency Code	Numeric	Yes	414
Transaction id	Numeric	Yes	Original transaction id
ZIP	Numeric	No	Should be kept empty
Address	Numeric	No	Should be kept empty
Member Detail	Numeric	No	Should be kept empty
Amount	Numeric (up to 3 decimal places)	Yes	Amount to be credited back to the cardholder
Track Id	Alphanumeric	No	Optional

UDF 1-5

Alphanumeric

No

Optional

- Merchant should upload the text file once it is ready, then **Convert > Validate > Upload**. If conversion or validation has failed, the reason would be a format issue; therefore ensure that there are no extra spaces, no extra lines at the top or end of the text file, and that the correct format is used.

Converted Successfully

Batch Upload

*Indicates mandatory field

Batch ID

Sample Format
Convert
Validate
Upload
Download Log

Validated Successfully

Batch Upload

*Indicates mandatory field

Batch ID

Terminal ID

Track ID

Sample Format
Convert
Validate
Upload
Download Log

Batch uploaded successfully

Batch Upload

*Indicates mandatory field

Input File*
Browse...

Sample Format
Convert
Validate
Upload
Download Log

- If the upload was successful, the batch report is viewed by navigating to **Reports > Batch Report**. Reports for processed batches can be viewed by navigating further to **View > Download** as shown below, which contains the list and result of each transaction processed through the same batch.



Title : Merchant Integration Manual

Version : 1.4

Doc : K-064

Date : 23 Aug. 2023

Section : Refund

Section : 7

Note: If batch status is “Not Processed” then the merchant has to contact the acquiring bank to start or schedule the batch at a later time. Once started, refunds will be processed.

Batch Report Menu:

Search By								
ALL								
Search								
S.No	Merchant ID	Terminal ID	Track ID	Batch ID	Transactions	Received Time	Status	Action
1	301	3010001	2099520450	1565172527309	2	Wed Aug 07 13:10:05 AST 2019	Not Processed	View
2	301	3010001	800673804	1564561646173	2	Wed Jul 31 11:27:48 AST 2019	Not Processed	View
3	301	3010002	45523613	1564555309391	1	Wed Jul 31 09:42:03 AST 2019	Processed	View
4	301	3010002	860384941	1564478411984	1	Tue Jul 30 12:20:23 AST 2019	Processed	View
5	301	3010002	521775803	1564469596431	3	Tue Jul 30 09:53:18 AST 2019	Processed	View
6	301	3010002	183141027	1564400784939	3	Mon Jul 29 14:46:33 AST 2019	Processed	View
7	301	3010002	530526808	1564393108004	3	Mon Jul 29 12:38:30 AST 2019	Processed	View
8	301	3010002	1627758157	1564389296348	3	Mon Jul 29 11:35:02 AST 2019	Processed	View
9	301	3010002	1100912675	1564388982587	3	Mon Jul 29 11:29:45 AST 2019	Processed	View
10	301	3010002	803015539	1563280622048	2	Tue Jul 16 15:37:05 AST 2019	Processed	View
11	301	3010002	2087325467	1563280569797	2	Tue Jul 16 15:36:14 AST 2019	Processed	View
12	301	3010002	1900685538	1563280085880	1	Tue Jul 16 15:28:11 AST 2019	Processed	View
13	301	3010002	573710736	1563279971680	1	Tue Jul 16 15:26:15 AST 2019	Processed	View
14	301	3010002	1965565335	1563279295638	522	Tue Jul 16 15:15:05 AST 2019	Processed	View
15	301	3010002	1692533618	1563278974004	1	Tue Jul 16 15:09:35 AST 2019	Processed	View

1 2 3 4

Batch Report

Merchant ID	301
Terminal ID	3010002
Track ID	45523613
Batch ID	1564555309391
Status	Processed
File Received Time	Wed Jul 31 09:42:03 AST 2019
Transactions	1
Process Start Time	Wed Jul 31 09:42:39 AST 2019
Process End Time	Wed Jul 31 09:43:39 AST 2019
Processed	1

Download

Back

8. Certification

Once integration is done, KNET will go through a testing process to certify a merchant's integration to the KNET Payment Gateway. On being officially certified, KNET will setup the terminal in the production environment, process the necessary paper work, and send them to the acquiring bank. The activation of the terminal in production is subject to the bank's approval only after the merchant is done with the final preparations.

The merchant must go through the below checklist that summarizes all the certification requirements that have to be completed by the merchant before initiating the certification test.

Note: *This is a generic certification checklist, which needs to be customized for each merchant.*

1. Merchant must import and install KNET CA certificates successfully on to their environment from the following URLs:
 - a. For testing environment: <https://www.kpaytest.com.kw>
 - b. For production environment: <https://www.kpay.com.kw>
2. Merchant integrates and communicates properly with Payment Gateway
 - Proper initialization of the plugin with the web page equivalent to “buy” demo page.
 - Ensure that the “PAY” button (on the page prior to redirection to the KNET payment page) can be clicked ONLY ONCE. This is to ensure that no duplicate transactions are initialized on clicking the button.
 - Ensure that a unique Track ID is generated by merchant in the payment request before redirecting to the KNET payment page. Each transaction should be initialized with a unique Track ID.
 - Ensure that the amount passed in the payment request matches the checkout page.
 - Redirecting customer to KNET payment page.
3. Merchant must provide KNET with an SSL certificate. The Merchant Support department is available to assist in this process on mail:PGSupport@knet.com.kw.
4. Merchant must present a receipt page after a successful OR unsuccessful transaction and display, at minimum, the following:
 - a. Date/time (Server Date & Time)
 - b. Transaction Result.
 - c. Amount
 - d. Payment ID
 - e. Merchant track ID

Merchant must send a notification email to the customer after a successful transaction and display, at minimum, the following:

- a. Date/time (Server Date & Time)
- b. Transaction Result.
- c. Amount
- d. Payment ID
- e. Merchant track ID

5. Merchant must present an error page after an unsuccessful transaction and display, at minimum, the following with clear notification of an unsuccessful transaction.

- a. Date/time (Server Date & Time)
- b. Transaction Result.
- c. Amount
- d. Payment ID
- e. Merchant track ID

6. Merchant MUST save all the records for all transactions, i.e.:

- a. Date/time (Server Date & Time)
- b. Transaction Result.
- c. Amount
- d. Payment ID
- e. Merchant track ID
- f. Transaction ID
- g. Reference ID
- h. Auth Code

8.1 Certification for KFAST

On opting for KFAST, it is the merchant's responsibility to ensure that he/she passes the correct and unique ReferenceNumber(Token) for each customer.

For the certification, the merchant will initiate a request, after which a time slot will be given to the merchant by the PGSupport team, wherein they will configure a test card to generate and receive an OTP for the merchant to complete the KFAST registration process. Once the certification process has been completed, the configuration of OTP is removed from the test card.

KFAST Certification checklist:

- a. Register multiple cards under different ReferenceNumber(Token).
- b. Remove added cards.
- c. Perform transaction(s) using KFAST by passing **CORRECT** token(s).
- d. Perform transaction(s) using KFAST by passing **INCORRECT** token(s).
- e. Verify each user has their **own** ReferenceNumber(Token).
- f. Merchant should provide evidence of above test cases.

Once the KFAST certification is completed and the merchant has provided all the required evidence, the PGSupport team will confirm the status of the certification (if passed or not) to the merchant, and enable the service if passed. This evidence will be saved by the PGSupport Team for later reference.

9. Troubleshooting Reference

9.1 Errors in initialization or inquiry

9.1.1 In case of Library based integration

Description: An error occurs when the PerformPaymentInitializationHTTP() or PerformTransaction() methods are called, or a non-zero value is returned, indicating a problem

Resolution is to ensure that:

1. The Alias is set correctly as defined in the merchant portal
2. The resource & key store files exist in the referenced path
3. The resource & key store file is defined correctly in full absolute form e.g. (D:\\Windows\\Resource\\)
4. The iPayPipe DLL is properly referenced in the project (in case of ASP.NET)
5. Reachability from client server to www.kpaytest.com.kw and www.kpay.com.kw through port 443 (telnet to these ports or browse these links locally from client server)
6. KNET CA certificates are installed on merchant trust store to ensure successful handshake when using inquiry.
7. UDFs & Track ID do not contain hack characters. Following is a list of the hack characters:

Field	Sym
UDF 1-5	@, /
Track ID	~, [,], /, ?, .

9.1.2 In case of RAW based integration

Description: A secure connection error returned after redirecting to KNET.

Resolution is to ensure that:

1. The Tran Portal ID, Tran Portal Password & Terminal Resource Key is defined correctly
2. The Merchant redirecting to the correct environment (test / production) depending

on the details defined in the above point

Note: The Merchant Support department is available to assist in the integration process on mail:PGSupport@knet.com.kw.

9.2 Not Receiving the Response Notification

9.2.1 Auto-void issue or notification response not reaching merchant server, namely responseURL.

Resolution is to ensure that:

1. Merchant response URL is defined in https and is publicly accessible through outgoing internet.
2. The merchant response page has a valid SSL certificate.
3. The KNET team is informed of any SSL updates or changes few days prior.
4. The merchant response page has no errors or html tags as output.
5. The merchant response page output is in the correct format (REDIRECT=<Merchant Receipt URL>.
6. The response page does not perform any redirections, instead the response page output is only the text line REDIRECT=<Merchant Receipt URL>. KNET PG will read the output line, extract the URL part and redirect the client's browser to that URL.

10. Error Codes and Description:

Error Code	Error Description
IPAY0100001	Missing error URL
IPAY0100002	Invalid error URL
IPAY0100003	Missing response URL
PAY0100004	Invalid response URL
IPAY0100005	Missing tranportal ID
IPAY0100006	Invalid tranportal ID
IPAY0100007	Missing transaction data
IPAY0100008	Terminal not enabled
IPAY0200001	Problem occurred while getting terminal
IPAY0100009	Institution not enabled
IPAY0200002	Problem occurred while getting institution details
IPAY0100010	Institution has not enabled for the encryption process
IPAY0200003	Problem occurred while getting merchant details
IPAY0100011	Merchant has not enabled for encryption process
IPAY0100012	Empty terminal key
IPAY0100013	Invalid transaction data
IPAY0100014	Terminal Authentication requested with invalid tranportal ID data
IPAY0100015	Invalid tranportal password
IPAY0100016	Password security not enabled
IPAY0200004	Problem occurred while getting password security rules
IPAY0200005	Problem occurred while updating terminal details
IPAY0100018	Terminal password expired
IPAY0200006	Problem occurred while verifying tranportal password
IPAY0100020	Invalid action type
IPAY0100022	Invalid currency
IPAY0100023	Missing amount
IPAY0100025	Invalid amount or currency
IPAY0100026	Invalid language ID

IPAY0100028	Invalid user defined field1
IPAY0100029	Invalid user defined field2
IPAY0100031	Invalid user defined field4
IPAY0100032	Invalid user defined field5
IPAY0100033	Terminal action not enabled
IPAY0100034	Currency code not enabled
IPAY0100035	Problem occurred during merchant hashing process
IPAY0100036	UDF Mismatched
IPAY0100038	Unable to process the request
IPAY0100039	Invalid payment id
IPAY0200009	Problem occurred while getting payment details
IPAY0100041	Payment details missing
IPAY0100042	Transaction time limit exceeds
IPAY0200011	Problem occurred while getting IP block details
IPAY0100043	IP address is blocked already
IPAY0100044	Problem occurred while loading payment page
IPAY0100045	Denied by Risk
IPAY0200013	Problem occurred while updating description details in payment log
IPAY0100047	Payment Page validation failed due to invalid Order Status
IPAY0100049	Transaction declined due to exceeding OTP attempts
IPAY0200015	Problem occurred while getting terminal details
IPAY0100050	Invalid terminal key
IPAY0100051	Missing terminal key
IPAY0100053	Problem occurred while processing direct debit
IPAY0100054	Payment details not available
IPAY0100056	Instrument not allowed in Terminal and Brand
IPAY0200016	Problem occurred while getting payment instrument.
IPAY0200018	Problem occurred while getting transaction details
IPAY0100057	Transaction denied due to invalid processing option action code
IPAY0100058	Transaction denied due to invalid instrument

IPAY0100059	Transaction denied due to invalid currency code
IPAY0100060	Transaction denied due to missing amount
IPAY0100061	Transaction denied due to invalid amount
IPAY0100062	Transaction denied due to invalid Amount/Currency
IPAY0100063	Transaction denied due to invalid track ID
IPAY0100064	Transaction denied due to invalid UDF1
IPAY0100065	Transaction denied due to invalid UDF2
IPAY0100066	Transaction denied due to invalid UDF3
IPAY0100067	Transaction denied due to invalid UDF4
IPAY0100068	Transaction denied due to invalid UDF5
IPAY0100069	Missing payment instrument
IPAY0100070	Transaction denied due to failed card check digit calculation
IPAY0100071	Transaction denied due to missing CVD2
IPAY0100072	Transaction denied due to invalid CVD2
IPAY0100073	Transaction denied due to invalid CVV
IPAY0100074	Transaction denied due to missing expiry year
IPAY0100075	Transaction denied due to invalid expiry year
IPAY0100076	Transaction denied due to missing expiry month
IPAY0100077	Transaction denied due to invalid expiry month
IPAY0100078	Transaction denied due to missing expiry day
IPAY0100079	Transaction denied due to invalid expiry day
IPAY0100080	Transaction denied due to expiration date
IPAY0100081	Card holder name is not present
IPAY0100082	Card address is not present
IPAY0100083	Card postal code is not present
IPAY0100084	AVS Check : Fail
IPAY0100085	Electronic Commerce Indicator is invalid
IPAY0100086	Transaction denied due to missing CVV
IPAY0100087	Card pin number is not present
IPAY0100088	Empty mobile number
IPAY0100089	Invalid mobile number

IPAY0100091	Invalid MMID
IPAY0100092	Empty OTP number
IPAY0100093	Invalid OTP number
IPAY0100095	Terminal inactive
IPAY0100096	IMPS for Institution Not Active for Transaction request, Institution :
IPAY0100098	Terminal Action not enabled for Transaction request, Terminal "termid" ,Tran Action : "action",-'opted action was not supported by that terminal
IPAY0100099	Terminal Payment Instrument not enabled for Transaction request, Terminal "termid" , Tran Instrument : "PAYMENT_INSTRUMENT"
IPAY0100100	Problem occurred while authorizing Transaction
IPAY0200019	Problem occurred while getting risk profile details
IPAY0100102	Denied by risk : Maximum Floor Limit Check - Fail
IPAY0100103	Transaction denied due to Risk : Maximum transaction count
IPAY0100104	Transaction denied due to Risk : Maximum processing amount
IPAY0200022	Problem occurred while getting currency
IPAY0100105	Action type not supported by maestro brand
IPAY0100106	Invalid payment instrument
IPAY0200024	Problem occurred while getting brand rules details
IPAY0100107	Instrument not enabled
IPAY0200025	Problem occurred while getting terminal details.
IPAY0100109	Invalid subsequent transaction, payment id is null or empty
IPAY0200026	Problem occurred while getting transaction log details
IPAY0200027	Missing encrypted card number
IPAY0100111	Card decryption failed
IPAY0100113	"transaction id" is a subsequent transaction, but original transaction id is invalid.
IPAY0100114	Duplicate Record
IPAY0100115	Transaction denied due to missing original transaction ID
IPAY0100116	Transaction denied due to invalid original transaction ID
IPAY0100118	Transaction denied due to card number length error

IPAY0100119	Transaction denied due to invalid card number
IPAY0100120	Transaction denied due to invalid payment instrument for brand data.
IPAY0100121	Transaction denied due to invalid card holder name
IPAY0100122	Transaction denied due to invalid address
IPAY0100123	Transaction denied due to invalid postal code
IPAY0100124	Problem occurred while validating transaction data
IPAY0100125	Payment instrument not enabled
IPAY0100126	Brand not enabled
IPAY0100127	Problem occurred while doing validate original transaction
IPAY0100128	Transaction denied due to Institution ID mismatch
IPAY0100129	Transaction denied due to Merchant ID mismatch
IPAY0100130	Transaction denied due to Terminal ID mismatch
IPAY0100131	Transaction denied due to Payment Instrument mismatch
IPAY0100132	Transaction denied due to Currency Code mismatch
IPAY0100133	Transaction denied due to Card Number mismatch
IPAY0100134	Transaction denied due to invalid Result Code
IPAY0100135	Problem occurred while doing perform action code reference id (Validate Original Transaction)
IPAY0200028	Problem occurred while loading default institution configuration (Validate Original Transaction)
IPAY0100136	Transaction denied due to previous capture check failure (Validate Original Transaction)
IPAY0100138	Transaction denied due to capture amount versus auth amount check failure (Validate Original Transaction)
IPAY0100139	Transaction denied due to void amount versus original amount check failure (Validate Original Transaction)
IPAY0100140	Transaction denied due to previous void check failure (Validate Original Transaction)
IPAY0100141	Transaction denied due to authorization already captured (Validate Original Transaction)

IPAY0100142	Problem occurred while validating original transaction
IPAY0200030	No external connection details for Extr Conn id :
IPAY0200031	Alternate external connection details not found for the alt Extr Conn id :
IPAY0100143	Transaction action is null
IPAY0200033	Problem occurred while getting vpas log details
IPAY0200034	Problem occurred while getting details from VPASLOG table
IPAY0100144	ISO MSG is null. See log for more details
IPAY0100145	Problem occurred while loading default messages in ISO Formatter
IPAY0100147	Problem occurred while formatting purchase request in B24 ISO Message Formatter
IPAY0100148	Problem occurred while hashing E-com PIN
IPAY0100150	Problem occurred while formatting Reverse purchase request in B24 ISO Message Formatter
IPAY0100152	Problem occurred while formatting authorization request in B24 ISO Message Formatter
IPAY0100153	Problem occurred while formatting Capture request in B24 ISO Message Formatter
IPAY0100155	Problem occurred while formatting reverse authorization request in B24 ISO Message Formatter
IPAY0100156	Problem occurred while formatting Reverse Capture request in B24 ISO Message Formatter
IPAY0100157	Problem occurred while formatting vpas capture request in B24 ISO Message Formatter
IPAY0100159	External message system error
IPAY0100160	Unable to process the transaction
IPAY0100162	Problem occurred while validating IMPS
IPAY0100163	Problem occurred during transaction
IPAY0100164	Transaction Not Processed due to Wrong ECI value
IPAY0100166	Transaction Not Processed due to Empty Authentication Status

IPAY0100167	Transaction Not Processed due to Invalid Authentication Status
IPAY0100168	Transaction Not Processed due to Empty Enrollment Status
IPAY0100169	Transaction Not Processed due to Invalid Enrollment Status
IPAY0100170	Transaction Not Processed due to invalid CAVV
IPAY0100171	Transaction Not Processed due to Empty CAVV
IPAY0200035	Amex Payment log details not available
IPAY0200036	Problem occurred while getting Amex payment log details
IPAY0100172	Problem occurred while converting amount
IPAY0100173	Problem occurred while building refund request
IPAY0100174	Problem occurred while calling Amex web service
IPAY0100175	Problem occurred in refund process
IPAY0100017	Inactive terminal
IPAY0100019	Invalid log in attempt
IPAY0100021	Missing currency
IPAY0100024	Invalid amount
IPAY0100027	Invalid track id
IPAY0100030	Invalid user defined field3
IPAY0200007	Problem occurred while validating payment details
IPAY0200008	Problem occurred while verifying payment details
IPAY0100037	Payment id missing
IPAY0100040	Transaction in progress in another tab/window
IPAY0200010	Problem occurred while updating payment details
IPAY0200012	Problem occurred while updating payment log IP details
IPAY0100046	Payment option not enabled
IPAY0100048	Cancelled
IPAY0200014	Problem occurred during merchant response
IPAY0100052	Problem occurred during merchant response encryption
IPAY0100055	Invalid Payment Status
IPAY0200017	Problem occurred while getting payment instrument list
IPAY0100090	Empty MMID
IPAY0100094	Sorry, this instrument is not handled

IPAY0100097	IMPS for Terminal Not Active for Transaction request, Terminal.
IPAY0100101	Denied by risk: Risk Profile does not exist
IPAY0200020	Problem occurred while performing transaction risk check
IPAY0200021	Problem occurred while performing risk check
IPAY0200023	Problem occurred while determining payment instrument
IPAY0100108	Perform risk check: Failed
IPAY0100110	Invalid subsequent transaction, Tran Ref id is null or empty.
IPAY0100112	Problem occurred in method loading original transaction data (card number, exp month / year) for orig_tran_id
IPAY0100117	Transaction denied due to missing card number.
IPAY0100137	Transaction denied due to credit amount greater than auth amount check failure (Validate Original Transaction)
IPAY0200029	Problem occurred while getting external connection details.
IPAY0200032	Problem occurred while getting external connection details for Extr Conn id
IPAY0100146	Problem occurred while encrypting PIN
IPAY0100149	Invalid PIN Type
IPAY0100151	Problem occurred while formatting Credit request in B24 ISO Message Formatter
IPAY0100154	Problem occurred while formatting Reverse Credit request in B24 ISO Message Formatter
IPAY0100158	Host timeout

IPAY0100161	Merchant is not allowed for encryption process
IPAY0100165	Transaction Not Processed due to Empty ECI value
IPAY0100176	Decrypting transaction data failed
IPAY0100177	Invalid input data received
IPAY0100178	Merchant encryption enabled
IPAY0100179	IVR not enabled
IPAY0100180	Authentication not available
IPAY0100181	Card encryption failed
IPAY0200037	Error occurred while getting Merchant ID
IPAY0100182	Vpas merchant not enabled
IPAY0200038	Problem occurred while getting vpas merchant details
IPAY0100183	Error occurred Due to byte PAREq is null
IPAY0100184	Error occurred while Parsing PAREq
IPAY0100185	Problem occurred while authentication
IPAY0100186	Encryption enabled
IPAY0100187	Customer ID is missing for Faster Checkout
IPAY0100188	Transaction Mode(FC) is missing for Faster Checkout
IPAY0100189	Transaction denied due to brand directory unavailable
IPAY0200039	Problem occurred while getting Faster Checkout details
IPAY0100190	Transaction denied due to Risk : Maximum transaction count
IPAY0100191	Denied by risk : Negative Card check - Fail
IPAY0100192	Transaction Not Processed due to Empty XID
IPAY0100193	Transaction Not Processed due to invalid XID
IPAY0100202	Error occurred in Determine Payment Instrument
IPAY0100194	Transaction denied due to Risk : Minimum Transaction Amount processing
IPAY0100195	Transaction denied due to Risk : Maximum credit processing amount
IPAY0100196	Transaction denied due to Risk : Maximum processing amount
IPAY0100197	Transaction denied due to Risk : Maximum debit amount
IPAY0100198	Transaction denied due to Risk : Transaction count limit exceeded for the IP

IPAY0100199	Transaction denied due to previous credit check failure (Validate Original Transaction)
IPAY0100200	Denied by risk : Negative BIN check - Fail
IPAY0100201	Denied by risk: Declined Card check – Fail
IPAY0100203	Problem occurred while doing perform transaction
IPAY0100204	Missing payment details
IPAY0100205	Problem occurred while getting PARES details
IPAY0100206	Problem occurred while getting currency minor digits
IPAY0100207	BIN range not enabled
IPAY0100208	Action not enabled
IPAY0100209	Institution config not enabled
IPAY0100210	Problem occurred during veres process
IPAY0100211	Problem occurred during pareq process
IPAY0100212	Problem occurred while getting veres
IPAY0100213	Problem occurred while processing the hosted transaction request
IPAY0100214	Problem occurred while verifying tranportal id
IPAY0100215	Invalid tranportal id
IPAY0100216	Invalid data received
IPAY0100217	Invalid payment detail
IPAY0100218	Invalid brand id
IPAY0100219	Missing card number
IPAY0100220	Invalid card number
IPAY0100221	Missing card holder name
IPAY0100222	Invalid card holder name
IPAY0100223	Missing cvv
IPAY0100224	Invalid cvv
IPAY0100225	Missing card expiry year
IPAY0100226	Invalid card expiry year
IPAY0100227	Missing card expiry month
IPAY0100228	Invalid card expiry month
IPAY0100229	Invalid card expiry day

IPAY0100230	Card expired
IPAY0100231	Invalid user defined field
IPAY0100232	Missing original transaction id
IPAY0100233	Invalid original transaction id
IPAY0100234	Problem occurred while formatting Reverse Capture request in VISA ISO Message Formatter
IPAY0100235	Problem occurred while formatting Reverse Credit request in VISA ISO Message Formatter
IPAY0100236	Problem occurred while formatting Reverse Credit request in VISA ISO Message Formatter
IPAY0100237	Problem occurred while formatting Reverse purchase request in VISA ISO Message Formatter
IPAY0100238	Problem occurred while formatting Capture request in VISA ISO Message Formatter
IPAY0100239	Problem occurred while formatting authorization request in VISA ISO Message Formatter
IPAY0100240	Problem occurred while formatting Credit request in VISA ISO Message Formatter
IPAY0100241	Problem occurred while formatting purchase request in VISA ISO Message Formatter
IPAY0100242	RC_UNAVAILABLE
IPAY0100243	NOT SUPPORTED
IPAY0100244	Payment Instrument Not Configured
IPAY0100245	Problem occurred while sending/receiving ISO message
IPAY0100246	Problem occurred while doing perform ip risk check
IPAY0100247	PARES message format is invalid
IPAY0100248	Problem occurred while validating PARES message format
IPAY0100249	Merchant response URL is down
IPAY0100250	Payment details verification failed
IPAY0100251	Invalid payment data
IPAY0100252	Missing veres
IPAY0100253	Problem occurred while cancelling the transaction

IPAY0100254	Merchant not enabled
IPAY0100255	External connection not enabled
IPAY0100256	Payment encryption failed
IPAY0100257	Brand rules not enabled
IPAY0100258	Certification verification failed
IPAY0100259	Problem occurred during merchant hashing process
IPAY0100260	Payment option(s) not enabled
IPAY0100261	Payment hashing failed
IPAY0100262	Problem occurred during VEREQ process
IPAY0100263	Transaction details not available
IPAY0100264	Signature validation failed
IPAY0100265	PARES validation failed
IPAY0100266	Brand directory unavailable
IPAY0100267	PARES status not successful
IPAY0100268	3d secure not enabled for the brand
IPAY0100269	Invalid card check digit
IPAY0100270	pares not successful
IPAY0100271	Problem occurred while formatting purchase request in MASTER ISO Message Formatter
IPAY0100272	Problem occurred while validating xml message format
IPAY0100273	Problem occurred while validation VERES message format
IPAY0100274	VERES message format is invalid
IPAY0100275	Problem occurred while formatting Credit request in MASTER ISO Message Formatter
IPAY0100276	Problem occurred while formatting Reverse purchase request in MASTER ISO Message Formatter
IPAY0100277	Problem occurred while formatting Reverse Credit request in MASTER ISO Message Formatter
IPAY0100278	Problem occurred while formatting reverse authorization request in MASTER ISO Message Formatter
IPAY0100279	Problem occurred while formatting Reverse Capture request in MASTER ISO Message Formatter

IPAY0100280	Problem occurred while formatting Capture request in MASTER ISO Message Formatter
IPAY0100281	Transaction Denied due to missing Master Brand
IPAY0100282	Transaction Denied due to missing Visa Brand
IPAY0200040	Problem occurred while performing card risk check
IPAY0200041	Problem occurred while getting institution configuration
IPAY0200042	Problem occurred while getting brand
IPAY0200043	Problem occurred while getting bin range details
IPAY0200044	Problem occurred while adding transaction log details
IPAY0200045	Problem occurred while updating VPASLOG table
IPAY0200046	Unable to update VPASLOG table, payment id is null
IPAY0200047	Problem occurred while getting details from VPASLOG table for payment id
IPAY0200048	Problem occurred while getting details from VPASLOG table
IPAY0200049	Card number is null. Unable to update risk factors in negative card table & declined card table
IPAY0200050	Problem occurred while updating risk in negative card details
IPAY0200051	Problem occurred while updating risk in declined card table
IPAY0200052	Problem occurred while updating risk factor
IPAY0200053	Problem occurred while updating payment log currency details
IPAY0200054	Problem occurred while inserting currency conversion currency details
IPAY0200055	Problem occurred while updating currency conversion currency details
IPAY0200068	Problem occurred while validating IP address blocking
IPAY0200069	Problem occurred while updating payment log card details
IPAY0200070	Problem occurred while updating ipblock details
IPAY0200071	Problem occurred during authentication
IPAY0200072	Payment log details not available
IPAY0100284	Invalid subsequent transaction, track id is null or empty
IPAY0100285	Transaction denied due to invalid original transaction
IPAY0100286	Unknown IMPS Tran Action Code encountered

IPAY0100287	Terminal Action not enabled for Transaction request, Terminal
IPAY0200056	Problem occurred while getting brand details
IPAY0200057	Problem occurred while getting external connection details
IPAY0200058	Problem occurred while updating message log 2fa details
IPAY0200059	Problem occurred while updating vpas details
IPAY0200060	Problem occurred while adding vpas details
IPAY0200061	Problem occurred during batch 2fa process
IPAY0200062	Problem occurred while getting brand rules details
IPAY0200063	Problem occurred while updating payment log process code details
IPAY0200064	Problem occurred while updating payment log process code and ip details
IPAY0200065	Problem occurred while updating payment log description details
IPAY0200066	Problem occurred while updating payment log instrument details
IPAY0200067	Problem occurred while updating payment log udf Fields
IPAY0100288	Terminal Payment Instrument not enabled for Transaction request, Terminal: termId, Tran Instrument: instrument name
IPAY0100289	Transaction denied due to Risk: Maximum credit amount
IPAY0100283	Problem occurred in determine payment instrument

11. Sample Demo Page Navigation

Step 1: Merchant Product Page

When a customer visits a merchant website, the merchant will display the products page for online shopping.

ONLINE SHOPPING




Price 15.KD
Qty
Add To Cart ☒



Price 10.KD
Qty
Add To Cart ☒



Price 20.KD
Qty
Add To Cart ☒



Price 25.KD
Qty
Add To Cart ☒

Step 2: Merchant Checkout Page

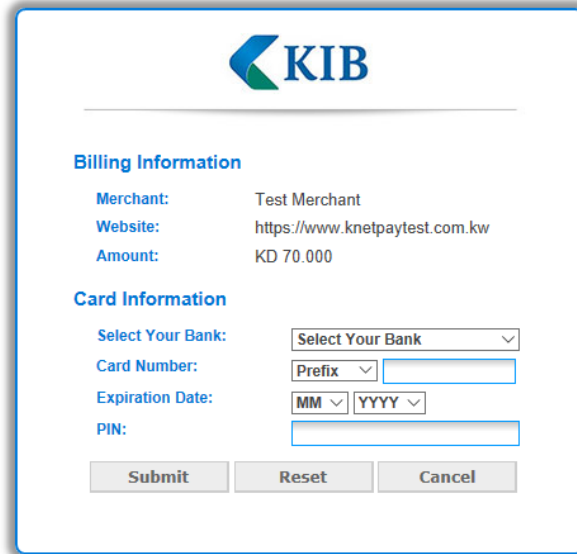
The customer shops, and items are added to the cart.

PRODUCTS ADDED TO CART

Product	Unit Price	Quantity	Price
Camay Soap	15	1	15
Cinthol Soap	10	1	10
Dettol Soap	20	1	20
Dove	25	1	25
Total Price			70.00 (KD)

Step 3: KNET Payment Page

Once the customer clicks on “Buy”, the KNET Payment Gateway page will be displayed to the customer. On this page, customers have to fill in their card details for payment processing.



The form is titled "KIB" and contains two main sections: "Billing Information" and "Card Information".

Billing Information:

- Merchant: Test Merchant
- Website: https://www.knetpaytest.com.kw
- Amount: KD 70.000

Card Information:

- Select Your Bank:
- Card Number:
- Expiration Date:
- PIN:

Buttons: Submit, Reset, Cancel

[Accepted Cards](#) | [KNET Home](#) | [Help](#)
[Copyrights](#) | [Privacy Policy](#) | [Disclaimer](#) | [View Certificate](#) | [Contact Us](#)

Driven by       @knetkw

Step 4: Merchant Receipt Page

After the transaction is processed by KNET, the customer is redirected back to the merchant website with the transaction response details.

Transaction Completed Successfully
Thank You For Your Order

Transaction Details (from Merchant Notification Message)	
Payment ID :	772481071492180
Post Date :	0807
Result Code :	CAPTURED
Transaction ID :	8836322071492180
Auth :	511212
Track ID :	3434
Ref No :	921814287057
UDF1 :	
UDF2 :	0412
UDF3 :	
UDF4 :	
UDF5 :	
UDF5 :	

12. Best Practices

12.1 Mandatory

- a) The Merchant must maintain logs for each transaction as mentioned below:
 - i. The parameters before setting the values in the respective variable.
 - ii. Request from the merchant server to Payment Gateway
 - iii. Response that is received from Payment Gateway in the Merchant Response URL
- b) The Merchant must complete the UAT and ensure all results are in line with the recommended response prior to going LIVE.
- c) Any changes in the pages would need to be tested before moving to Production after proper communication with the Bank personnel and receipt of approval. If the pages have a change in logic or transaction flow particularly, consent from the Acquiring Bank is mandatory.

12.2 Recommended

- a) It is essential for the transaction logs to be maintained in a secure storage location within the environment. This is crucial in order to trace transaction history in case of a dispute raised by a customer or even internal audit purposes. These logs should ideally include the customer IP address as well apart from the other transaction details.
- b) The Merchant should maintain "OWASP" (Open Web Application Security Project) Top 10 recommendation in their web application. (These recommendations are available on www.owasp.org)
- c) The Merchant should have the latest SSL security certificate in the payment request and receive webpage, if any. Always ensure that the SSL certificate is valid and has not expired. Such certificates should be as per the approved list of the Acquiring Bank. Self signed certificates are not supported by Payment Gateway in Test and Production Environment.
- d) The Merchant can use the inquiry feature to check the status of incomplete orders.
- e) The transaction request and Response Handling: For ease in integration, "Sample/Demo pages" provided in the integration document are essentially for

representation purposes only. The actual pages have to be necessarily developed and implemented by the Merchant's development team and used in both the Test and Production environment. The Sample demo pages are provided for the logical understanding and transaction flow only. An ideal logical flow for the merchant to process the customer input data is to collect the shopping details of the customer such as transaction amount, merchant track id and other parameters and stored in a secure storage location and validated immediately against the details of shopping cart module.



Title : **Merchant Integration Manual**

Version : 1.1

Doc : K-064

Date : 01 Jan. 2021

Section : Document Update Notice

Section : 13

13 Document Update Notice

Revision – 01

Reason for Change: ~~Document re-issue for the new PG and new services added~~
~~Version 1.1 – 2021 (Refund)~~



Title : **Merchant Integration Manual**

Version : 1.2

Doc : K-064

Date : 06 Feb. 2022

Section : Document Update Notice

Section : 13

Revision — 02

~~Reason for Change: Annual Review (2022)~~





Title : **Merchant Integration Manual**

Version : 1.3

Doc : K-064

Date : 27 Dec. 2022

Section : Document Update Notice

Section : 13

Revision – 03

Reason for Change: _____ Addition of Section 8.1
_____ (Certification for KFAST)

