

Payment Gateway

Integration Guide

PG Hosted

Version 0.1

Date: 14/11/2023

Copyright

©2023-24. PAYINONECLICK All rights reserved.

The material contained in this guide is copyrighted and owned by PAYINONECLICK together with any other intellectual property in such material. No part of this guide may be copied, republished, performed in public, broadcast, uploaded, transmitted, distributed, modified, or dealt with in any manner at all, without the prior written permission of PAYINONECLICK, and only in such a way that the source and intellectual property rights are acknowledged.

To the maximum extent permitted by law, PAYINONECLICK shall not be liable to any person or organization, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained in this guide.

The information in this material is subject to change without any prior notice. PAYINONECLICK assumes no responsibility for any errors.

Version Control Table

Date Updated	Version	Description of Changes	Author	Approved By
14/11/2023	0.1	Initial version	PAYINONECLICK Team	PAYINONECLICK

<u>1 ABOUT THIS GUIDE</u>	<u>5</u>
OBJECTIVES AND TARGET AUDIENCE	5
RELATED DOCUMENTATION	5
CONVENTIONS USED IN THIS GUIDE	5
Table 1: List of conventions	5
<u>2 INTRODUCTION</u>	<u>6</u>
PRE-REQUISITE	6
CONNECTING TO THE PAYMENT GATEWAY	7
Figure 1. PAYINONECLICK transaction flow	7
<u>3 PAYMENT PROCESS</u>	<u>8</u>
REDIRECTING CUSTOMERS TO THE PAYINONECLICK GATEWAY (STEP 1)	8
HOW TO REDIRECT THE CUSTOMER	8
TIPS FOR IMPROVING THE CUSTOMER EXPERIENCE	8
REFUNDS AND STATUS ENQUIRY	8
<u>4 INTEGRATION WITH PAYINONECLICK PAYMENT GATEWAY</u>	<u>9</u>
REQUEST FORMAT	9
Table 2: PAYINONECLICK Gateway parameters	9
AMOUNT FORMAT	11
CODE INTEGRATION EXAMPLES	12
RESPONSE PARAMETERS	13
Table 3: Response parameters	13
VALIDATING THE RESPONSE	15
<u>5 GENERATING A SECURE HASH</u>	<u>16</u>
SHA-256 SIGNATURE	16
GETTING Merchant KEY/SALT	18
<u>6 GATEWAY OPTIONS AND RESPONSE</u>	<u>19</u>
RESPONSE CODE FOR VALID TRANSACTION	19
Table 4: Response Codes for Valid Transactions	19

RESPONSE CODE FOR INVALID TRANSACTION	20
<i>Table 5: Response Codes for Invalid/Error Transactions</i>	21
NOTE : PLEASE NOTE THAT IF YOU GET A RESPONSE CODE WHICH IS NOT LISTED HERE THEN CONSIDER THAT AS A FAILED TRANSACTION	21
PAYMENT METHOD CODES	22
<i>Table 6: Supported Payment Methods</i>	22
NOTE: THE LIST OF PAYMENT MODES TO BE ACTIVATED IN LIVE MAY VARY DEPENDING UPON APPROVAL FROM RESPECTIVE BANKS	25
SUPPORTED CURRENCY CODE	25
<i>Table 7: Supported Currency with Codes</i>	26
RESPONSE STATUS	26
<u>7 GLOSSARIES</u>	<u>27</u>
<i>Table 9: List of Important Conventions and Definitions</i>	27

1 ABOUT THIS GUIDE

Objectives and target audience

This guide is designed to provide detailed information on how to integrate PAYINONECLICK Payment on a Merchant Website. The guide covers the steps in the payment process and the information that needs to be passed from Merchant web servers to PAYINONECLICK, to enable PAYINONECLICK to process payments. Additional gateway integration options are also described.

Related documentation

You should use this guide together with the additional PAYINONECLICK Payment Gateway documents described below.

Guide	Description
API specification Doc	Details of all reconciliation and refund APIs

Conventions used in this guide

The table below lists some of the conventions used in this guide.

Table 1: List of conventions

Convention	Description
Reference	Indicates a reference to another section in this guide. For Example, refer to the Introduction
File path	Used to indicate a file path or folder structure.
Glossary	Glossary term

2 INTRODUCTION

The PAYINONECLICK Payment Gateway is a secured payment aggregator, where you redirect customers from your Website/Ecommerce/M-commerce platform to PAYINONECLICK payment page, users can make a payment using Credit Card/Debit Card/UPI/Internet Banking other payment options. The gateway collects customer payment details in a secured manner using standard HTML forms and processes the payment transaction.

After the payment is complete, the customer is returned to the merchant website and the merchant receives a real-time notification of the payment, which includes details of the transaction.

PRE-REQUISITE

It is expected that the users may go through the entire guide to understand the Integration Requirements though it is easy for people with technical understanding.

It is assumed that the Merchant doesn't have any specific business need for Capturing the Customer's Card Information on their website as additional regulatory requirements of having PCI DSS certification is mandatory for capturing Customer's Credit/Debit/Net banking information on Merchant websites.

All Card/Net banking information is captured seamlessly on PAYINONECLICK payment Gateway Page in a secured manner and transaction response is returned to the Merchant real time post processing of the transaction.

Connecting to the Payment Gateway

Connecting to the PAYINONECLICK Payment Gateway requires adding PAYINONECLICK as a payment method on your website's checkout or payment page. When your customer selects the payment option, you should ensure that they are redirected to the PAYINONECLICK Payment Gateway. At the same time, you will need to submit information about the payment, such as your account ID, amount to be paid and a few other required parameters.

You can use a standard HTML form to collect and pass payment and customer details to PAYINONECLICK. An example of an HTML form is shown in **section Code Integration Example**

A simplified illustration of the transaction flow is shown in **Figure 1** below.



Figure 1. PAYINONECLICK transaction flow

1. When the customer is ready to pay for goods or services on your website, they select the PAYINONECLICK payment option on your website.
2. The customer is redirected to the Payment page where the user selects the payment mode and proceeds with the payment.
3. Customers are redirected to the bank systems for additional bank authentication.
4. Cash receives the response of the transaction from the bank.
5. User is redirected back to merchant website
6. Customer gets to know the status of the transaction

Optional steps:

7. Merchant gets SMS/email notification about the transaction status.

8. Customer gets SMS/email notification about the transaction status.

3 Payment Process

Redirecting customers to the PAYINONECLICK Gateway (step 1)

When a customer is on the online checkout or payment page on your website, they should be presented with a **Pay by PAYINONECLICK** button.

How to redirect the customer

When the customer selects the PAYINONECLICK button, merchant website should post the HTML form containing the transaction details to PAYINONECLICK PG

The HTML form should contain the required input fields listed in **Table-2** below.

Tips for improving the customer experience

Any parameters that you pass through in your HTML form, such as customer name, email and phone details, will be pre-populated in the relevant fields on the PAYINONECLICK Payment Gateway, making it easier for the customer to complete the payment.

You can customize the appearance of the PAYINONECLICK Payment Gateway and fields displayed to customers, using the Gateway options described.

To maximize conversion, PAYINONECLICK recommends that you redirect customers to the PAYINONECLICK Payment Gateway in the same browser.

Refunds and Status enquiry

Please refer to the API document for refunds via API or merchant CRM manual for initiating refunds via PAYINONECLICK portal.

Also, merchants can do a status enquiry in real time or later on to get the exact status of the transaction and verification of response.

4 Integration with PAYINONECLICK Payment Gateway

Request Format

Please review the table below for details of the required and optional parameters that need to be included in your form. An example of a simple HTML form is provided.

Request URLs

Production: <https://secure.payduniya.in/>

Table 2: PAYINONECLICK Gateway parameters

Field name	Description	Required	Type^	Min	Max	Example
Merchant Details						
PAY_ID	Pay ID is a unique merchant identifier provided by PAYINONECLICK	YES	NU	16	16	160234578452178
ORDER_ID	Merchant reference number	YES	AN	12	16	ESN78452
RETURN_URL	Url of merchant website to get the response after transaction is processed	YES	AN	5	ANY	https://www.response.com
HASH	Unique value generated by SHA 256 hashing algorithm	YES	AN	ANY	ANY	7995156CE4C40C 44C41BECA3B9CE 09B9

Customer Details						
CUST_NAME	Customer name	NO	AN	1	150	John Pal
CUST_PHONE*	Customer phone	YES	NU	8	15	07417456565
CUST_EMAIL*	Customer email	YES	AN	6	120	john@test.com

Payment Details

AMOUNT**	Total Amount	YES	NU	3	12	100
----------	--------------	-----	----	---	----	-----

^Abbreviation NU - Numeric, CH – Character, AN – Alphanumeric

Code integration examples

The sample request that has to be posted to PAYINONECLICK PG is given below, which is the recommended method for connecting to the PAYINONECLICK Payment Gateway.

All the parameters are as per the request params (Table 2). The request is a combination of mandatory and non-mandatory parameters.

For managing the integrity of the request, the request must contain the HASH parameter and the process of generating HASH is mentioned in section 5.

Note: Merchants can contact the PG support team or refer to the website for a specific language or framework kit. The integration kits are designed to act as plug and play kits and enable the merchant to integrate PAYINONECLICK PG with minimal effort. Every kit has its own set of instructions to help merchants go live within minutes.

Response parameters

When the payment process is complete PAY 247 does HTTP post back with the details of the transaction to the RETURN_URL provided by the merchant in request. This is done with a standard HTTP POST request. In case the merchant does not receive the transaction repose a status enquiry request can be initiated.

Table 3 shows the parameters sent to merchant RETURN_URL:

Table 3: Response parameters

Field name	Description	Example value
CUST_NAME	Customer name	John Pal
AMOUNT	Total Sale Amount	100
ORDER_ID	Merchant reference number	ESN78452
PAY_ID	Pay ID is given by PAYINONECLICK	160234578452178
TRANSACTION_ID	Transaction Id generated by PAYINONECLICK to identify the current step	150611417421130
USER_TRANSACTION_ID	Transaction Id entered by user on PAYINONECLICK while doing payment	11223344
STATUS	transaction status	Success

TEXT MESSAGE	Response message for transaction status	SUCCESS
HASH*	Unique value generated by SHA 256 hashing algorithm	Sample response value "7995156CE4C40C44C41BECA3B9CE09B9". Merchant always needs to make sure that the value returned by PG is the same as the value generated by the merchant. If the values are different then the merchant should reject the transaction, as this can lead to man in the middle attack.
RRN	Bank reference number	789456132
STATUS	Transaction status	success/error
CUST_EMAIL	Echo back field	john@gmail.com
CUST_PHONE	Echo back field	
RETURN_URL	Merchant return URL in request	www.merchantsite.com/paymentresponse

- * Refer Table 4 & Table 5 for Response Message
- * Refer Generate secure hash

Validating the response

The merchant application must validate the transaction response in the status response. This can be done as follows:

1. A successfully captured transaction can only be confirmed by **STATUS='success' and AMOUNT match in request/response, and HASH match in response**. If the above condition does not fulfill the transaction is not successful, and the merchant will be responsible for any losses.
2. Match the response HASH that is present in the response against the merchant application calculated hash value using the response params. In case the merchant hash does not match that transaction must NOT be considered a successful transaction. For successful transactions STATUS is 'success' and HASH should be matching.
3. Call the status API and verify the same result as received in real time response.

The merchant technical team can implement the ignore case snippet in their system to avoid disconnect.

Once you have validated the transaction data you can process the transaction, for example, by dispatching the goods ordered.

Please Note: The above implementations are a mandate for all the merchants and in case of any discrepancy at the merchant's end the merchant will be liable for any losses.

5 Generating a secure hash

SHA-256 signature

The merchant code creates the Secure Hash value on the Transaction Request data. The Payment Server creates another Secure Hash value and sends it back to the merchant in the Transaction Response.

The Secure Hash is a hexadecimal encoded SHA-256 HMAC of a concatenation of all parameters and values. The concatenation of parameters takes the form of a set of name-value pairs, like the parameter string for an HTTP POST call.

Method of generating hash

To generate a Hash you need to make a request of all the required

parameters For example, if you want to pass the following name value pairs

in your request

```
PAY_ID=1507281443471000&ORDER_ID=SIGORD220920151610&AMOUNT=100
&CUST_NAME=Demo&CUST_EMAIL=demo@example.in&CUST_PHONE=1234567890&RETURN_URL=htt
p://merchant.com/store/response.jsp
```

Then you need to sort all the parameters in ascending order extract only values and add “|”

symbol as separator . The Output will be as follows

```
100|demo@example.in|Demo|1234567890|SIGORD220920151610|1507281443471000|http://merch
ant.com/store/response.jsp
```

Next step is to generate a Secret Key/Salt and append at the end of generated. After adding you will get the following output

```
100|demo@example.in|Demo|1234567890|SIGORD220920151610|1507281443471000|http://merch
ant.com/store/response.jsp|qbeg
```

After completing the above-mentioned process, you will have to call SHA 256 algorithm and pass the parameter string to the same and the SHA will return you the desired result as below

```
Hash value= 1a8515609df5a5098dba1d2d69d37b00290d984ae9fd7c66200e701f9978f835
```

After that you must append previously generated Salt again to the generated value, and you will get the result as hash value

```
Hash value = 1a8515609df5a5098dba1d2d69d37b00290d984ae9fd7c66200e701f9978f835qbeg
```

Now you must encrypt generated value using Merchant Key provided by PAYINONECLICK, and you will get the final result as hash value

Hash value =

Nb/5dZr8U0WySYg/4wBll0ZyTTxdSFXBzPf/6Yvxv5fozmMb7dSiTHvmIVc6igknOpBL9VuS/1czluaY5SjICQ+2
BpEn5NXvYa3UbA45ioA=

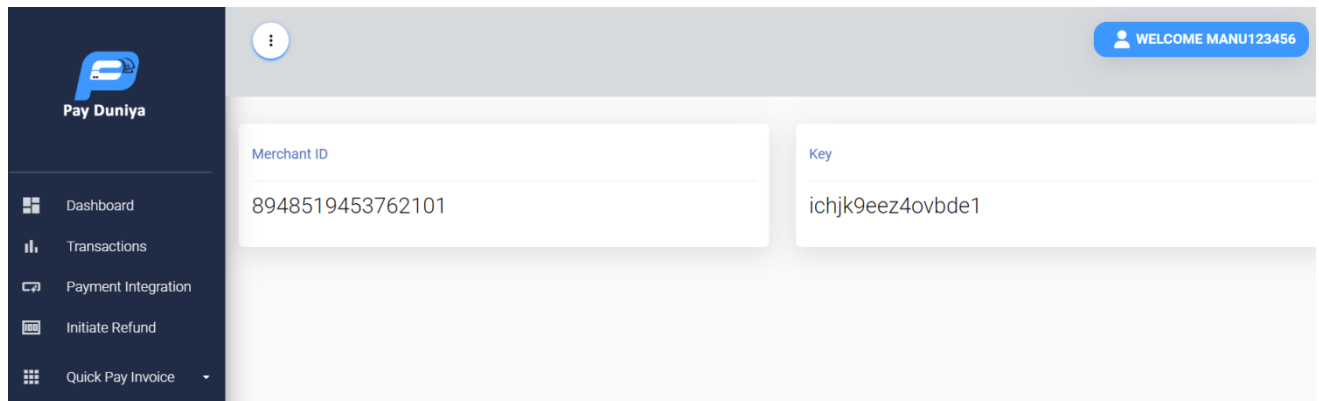
The purpose of the **SHA2 signature** field is to ensure the integrity of the data posted back to your server. You should always compare the **SHA2 signature** field's value posted by PAYINONECLICK's servers with the one you calculated.

To calculate the **SHA2 signature**, you need to take the values of the fields listed above exactly as they were posted back to you, concatenate them and perform a **SHA2** calculation on this string.

Getting Merchant key

The Merchant key is an essential element in generating hash. You have to encrypt the hash value with a key to generate the final hash through the SHA2 algorithm. You can find your merchant key in your merchant panel in following steps:

1. Login to your merchant account
2. Click on Payment Integration
3. You can find merchant key value under Integration Tab



6 GATEWAY OPTIONS AND RESPONSE

Response Code for Valid Transaction

Table 4: Response Codes for Valid Transactions

STATUS	Response message
success	Success
error	Duplicate
error	Canceled by user
error	Authorization success but error processing recurring payment
error	Denied due to fraud detection

Note: Please note that if you get a status which is not listed here then consider that as a failed transaction.

7 GLOSSARIES

This section provides a description of key terms used in this guide.

Table 9: List of Important Conventions and Definitions

Term	Explanation
Automated Payments Interface (API)	The API is a collection of tools that enables merchants to execute requests to the PAYINONECLICK Payment Gateway . For example: to send money, make 1-tap payments, check the status of transactions and download reports.
Browser	Application that enables a customer or merchant to access web pages. Examples include: Internet Explorer, Google Chrome and Mozilla Firefox.
Chargeback	The return of funds, previously authorized in a transaction, to a customer, which is initiated by their bank. The merchant may incur an administration cost for PAYINONECLICK processing the dispute, in addition to any amount eventually credited back to the customer.
Concatenation	Combining of multiple fields or parameters into a single text string or parameter.
Credit card	A type of payment card that allows customers to pay for goods and services using funds that are loaned. The loan must be paid back within a specified period. Interest is typically charged on the balance after a grace period (typically 20-55 days). Examples: Visa, MasterCard, Diners and Amex. See also Debit card .
Customer ID	Unique identifier for the customer or merchant's PAY 247 digital wallet account.
Customer services Team	PAY 247 team responsible for end-customer support queries. Also referred to as the PAY 247 Help Team . See also the Merchant Services team .
Debit card	A type of payment card that provides customers with instant access to funds in their bank account. Unlike credit cards , payments using a debit card are immediately taken from the customer's account,

	instead of being paid back at a later date. So, the customer must have sufficient funds in their account or an agreed overdraft limit to cover the payment.
Dynamic descriptor	An option that allows merchants to have their trading or brand name shown on the bank or credit card statement of the customer. The description can be changed on a per transaction basis. This option is Only supported for Visa, MasterCard.
HTML POST	Integration method where the merchant sends details to the PAYINONECLICK Payment Gateway using a standard HTML form that posts this information in the HTML header.
Iframe	HTML feature that enables the PAYINONECLICK Payment Gateway pages to be displayed within a frame on the merchant's website. The customer is not aware that they have been redirected to a third-party website.
Integration	Process undertaken by merchants to ensure that their website or

Term	Explanation
	a shopping cart can connect to and communicate with PAYINONECLICK.
ISO country codes	3-digit country code of the International Standards organization (ISO) that identifies the country. For example, GBR for the United Kingdom.
	ISO country codes also exist in a 2-digit format.
ISO currency codes	3-digit currency code of the International Standards Organization (ISO) that identifies the currency. For example, GBP for British Pound.
Merchant Services Team	PAYINONECLICK team responsible for providing technical and service support to merchants.
My Account	Merchant and customer account administration portal that enables viewing of transactions and transferring funds.
Payment option or Method	The payment method used by the customer, such as debit card, credit card and bank transfer. Note that in the payments industry, the terms payment method, payment option and payment type are often used interchangeably.
Payment page	Page used to collect payment method details from the customer during an online transaction.
Real-time	An event that occurs instantly or within a short period, such as seconds or minutes. For a real-time transaction, the customer, merchant or PAY 247 receive a response to the transaction request while the customer is still online.
Reason code	Every transaction has a reason code, which indicates the status of the transaction. PAY 247 receives a variety of reason codes from the bank or scheme authorizing the transaction and consolidates these before providing them to merchants.
Transaction	Each financial interaction on the system is referred to as a transaction.
PAY 247 Payment Gateway	PAY 247's secure page for processing transactions. Merchants connect to the Payment Gateway, which will then process transactions from their website.

Term	Explanation
Transaction	Each financial interaction with the PAYINONECLICK Payment Gateway is referred
	to as a transaction. Transactions are linked to payments .
Transaction ID	Unique ID assigned to a transaction by the PAYINONECLICK Payment Gateway .
PG_REF_NUM	Unique ID assigned to a transaction by the PAYINONECLICK Payment Gateway . This id is used for further communication with PAYINONECLICK Payment Gateway .
Transaction status	Each transaction on the PAYINONECLICK Payment Gateway is given a status. This
	includes: <i>processed, pending, temporary, scheduled, canceled, failed,</i>
	<i>charge backed successfully.</i>

**THIS PAGE IS INTENTIONALLY LEFT
BLANK**