IPG INTEGRATION DETAILS - Commercial Bank SandBox

The following methods are available to proceed with the integration. Visit the URL below for details.

Hosted checkout (Light Box)
Hosted Session
Direct Payment (for PCIDSS certificated entities)

Integration Guide - https://test-gateway.mastercard.com/api/documentation/integrationGuidelines/index.html?locale=en_US

Base URLs for initialing API calls: - https://cbcmpgs.gateway.mastercard.com/

Please use API version 100

Please keep cipher suites and TLS version 1.2

Please use the attachments below:

a) Test Credentials (password will be sent shortly)
b) Acquiring Bank logo
c) Card Acceptance logos
d) Authentication logos

MPGS also provides SDK for mobile Apps on both iOS & Android.

Mobile SDK Guide- https://test-gateway.mastercard.com/api/documentation/integrationGuidelines/mobileSDK/integrationModelMobileSDK.html?locale=en_US

Mobile SDK GIT HUB - https://github.com/Mastercard-Gateway

To run the demonstration app bundled within the SDK, you must host an instance of the demonstration PHP merchant server. The Mobile SDK uses the Update Session with Payer Data operation to pass card data from the mobile device to the gateway. This operation does not require authentication credentials because the Mobile SDK provides the sessionId in the URL context parameter. Please note that the merchant API password or certificate are secret and should never be inserted within a mobile app.

Please use API version 49

Further, to support the IPG in mobile Apps the merchant is expected to comply with the requirements / guidelines issued by Central Bank of Sri Lanka. Please refer the url

https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/psd_guideline_no_1_of_2020_e.pdf

IMPORTANT

The integration guide provides instructions on how to perform the IPG integration. It is the responsibility of the merchant /developer to design/develop the website in a secure manner considering all the aspects presented by integration guide. The philosophy of the design is at the discretion of the merchant/ web developer as it lies on the merchant's domain and is beyond the control of the IPG.

Merchant should carry out a comprehensive UAT and if needed Merchant may conduct a suitable vulnerability assessment of the development done. Merchant should understand that the security vulnerabilities/exploits depend heavily on various aspects such as programming tools, languages, libraries, plugins, databases, network and other factors that you may use and the Bank has no control over the implementation/design of these factors which are solely at the discretion of the merchant.

Please refer to the below.mentioned URL for test card details

https://test-gateway.mastercard.com/api/documentation/integrationGuidelines/supportedFeatures/testAndGoLive.html?locale=en_US