Getting started

This document describes how you can get started with development on the sandbox environment. Scroll to the bottom if you are looking for common use cases. Bookmark this page so you can easily find it later.

Documentation

There are two sources of documentation. The first source is portal you are on now. It has detailed descriptions of how to integrate into the different APIs. The second source is the API reference found at https://sandbox.omni.verifone.cloud/docs/api. The API reference has up to date descriptions of the various endpoints and parameters required for each endpoint.

Environments

There is a sandbox and a production environment. The data stored in the sandbox environment does not carry over to the production environment. This means that any API keys, organisation IDs, and user accounts that can be used in the sandbox environment will not work in the production environment. User accounts also need to be created in the sandbox and production environment.

Make sure the following values are configurable per environment:

- URL
- API Key
- Organisation ID
- Account ID(s) - One account per currency
- Authenticator ID(s) - One authenticator per MID-currency combination. The same authenticator can be used across multiple accounts if they have the same MID but a different currency.

URLs

URL	Description
https://verifone.cloud/docs/uk-gateway/getting-started	Integration documentation
https://sandbox.omni.verifone.cloud/docs/api	API Reference
Https://sandbox.omni.verifone.cloud/	Sandbox portal
https://sandbox.omni.verifone.cloud/v1/	Sandbox API
https://omni.verifone.cloud/	Production portal
https://omni.verifone.cloud/v1/	Production API

Account set up & API key

Your account will be set up for you by a Verifone employee. Your API key can be retrieved by following this guide. Once you have your key store it somewhere safe and make sure it is configurable, in production you will have a different API key. The API Key is tied to a users account, use an email that other employees also have access too. This way issues won't be caused when people leave the position or company.

Once your account has been set up you will receive the following:

- Organisation ID
- Account ID (1 per currency)
- Authenticator ID (if you are processing 3DS transactions)

Make sure these values are configurable as the IDs do not carry over to production.

Choosing an integration method

We offer three distinct methods for processing payments, methods might also need to be used together for processing specific payment journeys.

Each integration method has tradeoffs that need to be considered. Regardless of which integration method is chosen we advise to always supplement with API calls. The three options are:

- Checkout
- Inject
- API

Checkout

Using Checkout (Hosted Payment Page) to process payments will return a link to a hosted payment page. The webpage requires the cardholder to be redirected away from the webshop, after payment is completed the cardholder is returned to the webshop. Checkout allows for a fully customizable CSS file to be used to match the look and feel of the webshop. This solution offers less flexibility than a direct API integration but can make it easier to integrate with due to a lower level of PCI compliancy required. The consumer will enter their card details in the hosted payment page. This solution is easier to integrate than the direct API integration.

Inject

Using Inject means that a JavaScript snippet will need to be placed on your webshop that renders a payment form. This payment form provides fields where the customer can present their card details. After the card details are submitted a token is returned. This token needs be used to initiate the transaction through the API. This option has the benefit of using the flexible API, while not needing to meet the highest level of PCI compliancy. However, the JavaScript snippet will need to be implemented in the website, it can be changed but only to a certain degree. This is the most common integration method.

API

Using the API to process payments offers the highest level of flexibility and customization of the checkout flow. If you have the correct level of PCI compliancy this is always the preferred method of integration. Having full control allows you to fully optimize the checkout process and better integrate with your product or service. You will need the be compliant with SAQ C PCI compliancy as you will be submitting the card details through your own server.

Integration method	Flexibility	Implementation	PCI
Checkout	Medium	Redirect customer to hosted payment page	SAQ A

Integration method	Flexibility	Implementation	PCI
Inject	High	Render JS form + direct API calls	SAQ A-EP
API	High	Direct API Calls	SAQ C

3-D Secure

3-D Secure authentications can be processed through Checkout, Inject or using the API. Read more about 3-D Secure here.

For processing one-click payments (CoF) this is possible exclusively through the API. Tokenization and the inital transaction can be initiated through any of the integration methods (Checkout, Inject or API) but the follow-up transactions and 3-D Secure authentications can only be processed through the API.