

# **Getting Started: Integration**

Credit & Debit Card Processing

v 1.0.03

# Introduction

## Overview

This document is intended to give a non-technical overview of starting the integration process. The points of concern for this document are selecting the most appropriate integration method, and ensuring that the merchant has all the information and resources to allow their developer to quickly and easily integrate into the system.

This document covers the credit and debit card processing.

## Choosing an Integration Method

There are three integration methods that can be used to integrate into the payment system. The one that is most appropriate will depend on a number of factors. Our system doesn't make the merchant select which integration method can be used, and allows different integrations against the same Gateway Account to be in place simultaneously – there are certain situations which this will actually be necessary. Once you have reviewed the information below and decided on the most appropriate integration method for your needs, please refer to the integration specific documentation for the technical details on its implementation.

1. **Direct/API Integration** – Direct/API processing allows merchants to keep their customers on their site throughout the entire checkout process. This provides a much smoother checkout experience, and keeps the details of the underlying payment processor completely hidden from the customers. The API for this method exposes the full functionality of the payment system. This method requires the merchant's system to be able to serve out HTTPS pages, which will likely require them to have an SSL certificate.

**Difficulty:** 4/10. Of the integration methods, this is probably the easiest to implement, as well as giving you the most control of the transaction process.

**PCI-DSS SAQ\*:** SAQ-D

2. **Hosted Payment Form** – we can provide a secure payment form which the customer is redirected to during the checkout process. They will complete the order on our system and then be redirected back to the merchant's system with the results of the transaction. Our system allows this payment form to be completely re-skinned so that it closely matches the merchant's own branding. This method is generally used by merchants who are using a shopping cart that does not support the Direct/API integration method, merchants who cannot host secure (HTTPS) pages or merchants who would like to completely outsource the payment process of their website – usually for PCI compliance reasons.

**Difficulty:** 6/10. Because this integration uses the users browser as a data relay, there are some additional steps required to securely transmit the data to/from the payment gateway, as well as handling the response. These additional steps add complexity to the integration.

**PCI-DSS SAQ\*:** SAQ-A

3. **Hosted Payment Form (iFrame Mode)** – The Hosted Payment Form can be used in "iFrame" mode, which would allow it to be embedded into a payment form that is hosted on the merchant's system. The system will apply a different, cut-down skin to the Hosted Payment Form in this mode, which will only skin the direct form.

**Difficulty:** Intermediate. The integration is more or less identical to the Hosted Payment Form.

**PCI-DSS SAQ\*:** SAQ-A

4. **Hosted Fields** – the Hosted Fields integration method allows the merchant’s system to appear to keep the customer on their own system during the checkout process, but the sensitive fields are served transparently by the payment system through iFrames. This approximates the appearance and experience of the Direct/API method, but has the same compliancy requirements as the Hosted Payment Form method.

**Difficulty:** 6/10. Because this integration uses the users browser as a data relay, there are some additional steps required to securely transmit the data to/from the payment gateway, as well as handling the response. These additional steps add complexity to the integration.

**PCI-DSS SAQ\*:** SAQ-A

5. **Transparent Redirect** – the Transparent Redirect method allows the merchant’s system to appear to keep the customer on their own system during the checkout process, but the card details don’t actually touch the merchant’s system – they get posted directly across to the payment system. This approximates the appearance and experience of the Direct/API method, but it has the same compliancy requirements as the Hosted Payment Form method.

This method requires the merchant’s system to be able to serve out HTTPS pages, which will require them to have an SSL certificate.

**Difficulty:** 7/10. Because this integration uses the users browser as a data relay, there are some additional steps required to securely transmit the data to/from the payment gateway, as well as handling the response. These additional steps add complexity to the integration.

**PCI-DSS SAQ\*:** SAQ-A-EP

*\* assumes that your annual transaction count (or any other factor) allows your PCI-DSS compliance to be self-attested*

## Getting Started Checklist

Before you start your integration, please run through this checklist to ensure you have everything that you need.

1. **Access To The Merchant Management System (MMS)** – please check that you have access to the MMS. A merchant super user will have been automatically created when the account was initially created – the details of this account will have been emailed to the account owner. We recommend that a dedicated MMS User account be created for the developer – this has to be done by the account owner, and can be done from the Account Admin | User Admin page in the MMS. The MMS also has useful resources for the developer, and the transaction reporting section will allow the developer to view any transactions that they process as part of the integration testing. Please note – the MMS User account details are completely separate from the Gateway Account details.
2. **Latest Integration Documents** – please ensure that you have the latest version of the integration documents, which are available to download from the Support | Downloads section in the MMS.

3. **Latest Integration Code Pack** – we provide code packs for the most common web languages. For each language, we have written an integration library and a fully functional sample payment form. The sample payment forms have been designed to be reused wholesale with as little modification as possible, but in the event that this is not possible, they demonstrate how to make use of the underlying integration library, and so will still be a valuable resource. We recommend that the latest code pack be used. The code pack can be downloaded from the MMS
4. **Test Gateway Account Credentials** – on registration a test Gateway Account will have been created automatically. Details of this account would have been emailed to the account owner. Test Gateway Accounts run on exactly the same system as production Gateway Accounts, and are designed to mimic production accounts precisely. We recommend that merchants perform their integrations against their test Gateway Account. Please note – the Gateway Account details are completely separate from the MMS User account details.
5. **Additional Account Information** – if the Hosted Payment Form or Transparent Redirect integration method is selected, then the developer will require additional account details – namely, the Pre Shared Key, and elected Hash Method. These details can be found in the Account Admin | Account Settings page of the MMS. If you have created your developer their own MMS User account, then they should be able to access these details directly.
6. **Test Card Document** – a test Gateway Account will only work with the test card numbers detailed in this document (conversely, a production Gateway Account will only work with real card numbers). This document is available to download from the Support | Downloads section of the MMS.