Sensible Development

Payment integration

Date:

May 2012

Version:

1.1

Payment Systems

For many reasons, your auction website needs to be able to take payments. Most importantly, winning bidders will need to pay for the items they have won.

There are various particular ways in which we can integrate payment gateways with your auction website. The integration options fall into two main categories:

Off-site integration

Off-site integration, also known as "forms" type integration, is the quickest and easiest integration option. It means that users will have to be redirected to another website (e.g. PayPal) in order to enter their card details and pay for items. You will only be able to customise your payment page to a limited extent with this integration method. You will also not be able to automate transaction functions like refunding or repeating transactions. However, this method of integration is simple and inexpensive with very few potential security issues.

With this option there is no need to gather, store or process sensitive information on your website. The server never sees any credit card details. Instead we merely receive "tokens" from the payment gateway to indicate whether or not a payment has worked. Thus there is no obligation to pay for security certificates of any kind, or invest in costly PCI compliance.

API type integration

API stands for "application programming interface". API type integration means that the payment system will be fully integrated with your website. Therefore users will not have to leave your website in order to pay for items. You will also be able to perform automated transaction functions (like refunding, repeating and aborting transactions). This form of integration is very professional-looking, and allows a greater amount of control and adjustability in managing transactions than off-site integration does.

However, this option can incur some additional security-related costs. Any organisation with payment card data must meet the requirements of the PCI DSS (Payment Card Industry Data Security Standard). This is a set of security standards that aims to minimise the danger of people's card data being misused. As credit card details will be passing through the server, this means it is necessary to verify that the server is secure.

The server must be scanned for any potential security risks and must comply with PCI DSS's 12 compliance requirements. This does not involve a great deal more than ticking various boxes on a questionnaire to "prove" that the server is secure. Our software is fortunately built in such a way that we do not fall foul of most PCI compliance issues. However, there may still be some changes that need to be carried out and these can add extra costs to the entire process.

It should be noted that PCI compliance is more difficult and complicated for websites which run on shared servers, as there are more potential security issues. For this reason, off-site integration is possibly a better option to consider for such websites.

At Sensible Development, we work with three different internet payment gateways:

PayPal

PayPal is a global internet payment gateway. We provide integration with PayPal as part of our standard platform. PayPal performs payment processing for online vendors, auction sites and other commercial users, for which it charges a fee. PayPal is especially suitable for charity fundraisers as it can be used to distribute funds to sellers after taking a commission. It also has a low cost of entry. PayPal accepts payments in 20 major currencies.

There are three main payment/integration options with PayPal:

- **Website Payments Standard**, an off-site integration option for small or new businesses. This has no application or set up fees, or monthly charge, and takes just a matter of minutes to set up. Users will be diverted to the PayPal website to pay and once they have paid will be sent back to your website (to a page of your choice). As PayPal will be handling all the payment card information, you will not have any need to meet security compliance standards yourself.

- **Website Payments Pro**, an API type integration option for medium or established businesses (over £50, 000 a year online). With this option, the payment page will be securely hosted by PayPal but can be fully customised and branded so it looks identical to your website. Unless you choose the hosted version of Website Payments Pro, you will have full responsibility for your own PCI compliance. With **Website Payments Pro Hosted** PayPal takes responsibility for the processing and storing of card details, greatly diminishing the amount of PCI compliance you have to deal with.

- **Website Payments Pro with additional benefits**, an API type integration option for large businesses (over £1 million a year online). This option is essentially the same as Website Payments Pro but can be tailored to fit your specific needs, and has various added benefits such as a dedicated account manager.

SagePay

SagePay, formerly known as Protx, is a UK based internet payment gateway for UK and Republic of Ireland merchant accounts. It is the largest independent payment service provider in the UK. It accepts multiple currencies.

There are four main payment/integration options with SagePay:

- The **Form** option, an off-site integration method. This is the simplest way to begin processing online payments and takes just a few minutes to set up. Users will be diverted to the SagePay website to pay for items. All transaction information will be held at SagePay. The payment page can be customised with your company branding. Security-wise, the only requirements are that you take an online self-assessment security questionnaire.

- The **Server** option. This option is not dramatically different from Form. As with Form, users are redirected to SagePay's payment pages to enter their card details and SagePay deals with the transaction. However, although SagePay stores sensitive card data, other customer information is sent back for storage within your server. You do this without handling, collecting or storing sensitive card data yourself. The payment page can be customised with your company branding. Security-wise, the only requirements are that you take an online self-assessment security questionnaire.

- The **Server and InFrame** option. This option is very much the same as Server, but allows users to remain on your website while they enter their card data into SagePay's payment page. Thus buyers never leave your URL to pay for their item. With this option, you will be able to fully customise the branding and layout of the area outside of the payment fields. For security, you will be required to take an online self-assessment questionnaire and undergo regular vulnerability scanning.

- The **Direct** option, an API type integration option. With this option you will have your own secure payment page on your website on which users will enter their card details, and you will have full control over all aspects of the appearance of the page. You will have the ability to fully control the payment process to meet all of your requirements. There is a heavy security burden with this option, and you will have to pay for PCI DSS certification.

Authorize.net

Authorize.net is a USA based internet payment gateway for USA merchant accounts. Authorize.net has a user base of over 305,000 merchants, and is one of the internet's largest payment gateways.

There are three main payment/integration options with Authorize.net:

- **Direct Post Method**, an API type integration option. This option enables you to completely tailor the payment process, while at the same time giving full responsibility in handling transactions to Authorize.net.

- **Server Integration Method**, an API type integration option. With this option, Authorize.net will handle all transactions but you will be able to customise the appearance of the payment form to such an extent that Authorize.net's presence is almost unnoticeable.

- **Advanced Integration Method**, an API type integration option. This integration option allows you to host your own secure payment page on your website. You will have complete control over the payment process. There is a heavy security burden with this option, and you will have to pay for PCI DSS certification.

Call-backs

Once your payment gateway has received a payment, it will contact the relevant bank to validate if the payment has been successfully authorised, and will notify you of whether or not this is the case. These notifications are known as "call-backs". Call-backs will also inform you of any events that have occurred that affect a transaction. Call-backs are essential in order for you to be able to verify payments, send invoices and release items to winning bidders. Each payment gateway has its own slightly different call-back system.

PCI DSS

The Payment Card Industry Data Security Standard is a set of security standards that aims to minimise the danger of people's card data being misused. All organisations with payment card data must meet its requirements. However, the extent of compliance expected varies according to your PCI DSS compliance level. There are four compliance levels and which one applies to you depends on the volume of transactions your business processes. Businesses processing less than 20, 000 transactions a year are classified as Level 4 and have the lowest (and least costly) compliance requirements. Businesses processing over 6 million transactions a year are classified as Level 1 and have the highest compliance requirements.

The 12 PCI DSS compliance requirements, or "control objectives", are as follows:

1) Install and maintain a firewall configuration to protect cardholder data

2) Do not use vendor-supplied defaults for system passwords and other security parameters
3) Protect stored cardholder data
4) Encrypt transmission of cardholder data across open, public networks
5) Use and regularly update anti-virus software on all systems commonly affected by malware
6) Develop and maintain secure systems and applications
7) Restrict access to cardholder data by business need-to-know
8) Assign a unique ID to each person with computer access
9) Restrict physical access to cardholder data
10) Track and monitor all access to network resources and cardholder data
11) Regularly test security systems and processes
12) Maintain a policy that addresses information security