ProtectPay

ProtectPay is ProPay's tokenization solution. Tokenization provides security to merchants by replacing the need to store sensitive payment information with replacement data that offers no value to a would-be data thief. Real payment data is maintained in a secure vault, while merchants use the token to initiate transactions.

What are Payer Management Interfaces?

The ProtectPay Payer Management Interfaces (PMIs) are special controls used to further limit exposure of sensitive credit card data to the merchants who wish to process using ProtectPay.

While use of ProtectPay in itself can benefit customers who need to STORE sensitive data (by replacing that data with tokens) it is only by using a PMI that the customer benefits from all of what ProtectPay can offer.

Option 1: Hosted Payments Page

The hosted payments page (HPP) is a collection of utilities that allow merchants to place a page entirely hosted by ProPay on their own website.

Step 1: Use the ProtectPay API to define the nature of a Hosted Page. You will get back a page identifier.

Step 2: Place the HPP on your website while including the identifier in the HPP URL. The HPP will "ping" your site when it has collected payment.

Step 3: Collect success data associated with the page identifier.

The ProtectPay PMI: Hosted Payment Page is the preferred method of integration because it provides the most protection to cardholders and alleviates more PCI compliance burden than any other method.

Option 2: Seamless Payment Interface

The Seamless Payment interface (SPI) is a solution that allows merchants to create their own checkout page with absolute control over the user experience. In fact, the SPI includes no visual component, at all, hosted by ProPay. Here is how it works:

Step 1: Merchant's website "paints" a checkout page down to the cardholder's browser. This page must contain a "submit" button that executes client-side code.

Step 2: When a cardholder clicks the "submit" button, data from the checkout page is POSTed to the SPI. (This is not typical for web pages in that, usually, POSTs go back to the same website that serves up a page.)

Step 3: The SPI processes a transaction then redirects the cardholder's browser to a URL specified by the merchant in the POST. This redirect includes a payload to inform the merchant about the success or failure of the transaction.

The SPI is a great solution for merchants who want to control the entire checkout experience. However, it satisfies fewer PCI requirements and its use alleviates fewer PCI obligations.

Option 3: Frame-able control

The Frame-able control is kind of like a "stripped down" version of the HPP. The control will only collect credit card numbers and return tokens to a merchant. Merchants, then, can use these token in an API call to process transactions. All other information needed to process the card must be collected, maintained, and passed in the transaction request. (This even includes expiration dates. The control ONLY collect the card number.)

Option 4: Full Function Redirect

The Full Function Redirect has a very specific use-case and is only useful to a limited number of merchants. It actually allows cardholders to enter multiple cards into a wallet type solution.

Swipe: when PMIs will not work

As you may have noticed, all of these PMI solutions are suitable for ecommerce processing. Card-present solutions will ALWAYS put merchants "into scope" for the PCI-DSS because hardware must connect to a physical machine that is then, inevitably, going to handle sensitive data.

ProPay offers solutions for card present data security. Please see our best practices guide for mobile processing.

PROPAY
A TSYS® Company

For more information on how the flexible services of the ProPay Payment Network can help your organization reach its objectives, please call 1-888-227-9856 or visit www.propay.com.