**PHP 3 Party (Server Hosted) VPC SHA256 Example Code**

## What files are included in the package?

* PaymentCodesHelper.php
  + Contains functions that help modify response codes to text.
* VPCPaymentConnection.php
  + Contains functions to connect to the gateway and construct SHA256 HMAC.
* PHP\_VPC\_3Party\_Order.html
  + Displays the input fields required to complete the transaction
* PHP\_VPC\_3Party\_Order\_DO.php
  + Sorts POST data and sends Digital Order to the Payment Server
* PHP\_VPC\_3Party\_Order\_DR.php
  + Displays Digital Receipt data

## How do I change from MD5 to SHA 256?

Get your developer to look at your current code and locate where the MD5 hash is being calculated. They will need to look at the logic below and replace the current MD5 hash calculation with the below SHA256 HMAC calculation.

**Step 1: Create string with transaction data via the merchant application.**

Create a string with field names and values in ascending order using the POST data from PHP\_VPC\_3Party\_Order.html:

|  |
| --- |
| foreach($\_POST as $key => $value) {  // create the hash input and URL leaving out any fields that have no value  if (strlen($value) > 0) {  ?>  <input type="hidden" name="<?php echo($key); ?>" value="<?php echo($value); ?>"/><br>  <?php  if ((strlen($value) > 0) && ((substr($key, 0,4)=="vpc\_") || (substr($key,0,5) =="user\_"))) {  $hashinput .= $key . "=" . $value . "&";  }  } |

**Step 2: Create SHA256 HMAC**

* *Obtain Secure Hash Secret either from the existing MD5 calculation or from Merchant Administration*
* *Calculate SHA256 HMAC using the secret as a key to produce the secure hash*
* *Add the hash to the request string to send to the gateway*

|  |
| --- |
| }  $hashinput = rtrim($hashinput, "&");  ?>  <!-- attach SecureHash -->  <input type="hidden" name="vpc\_SecureHash" value="<?php echo(strtoupper(hash\_hmac('SHA256', $hashinput, pack('H\*',$securesecret)))); ?>"/>  <input type="hidden" name="vpc\_SecureHashType" value="SHA256"> |

## Can I process 2.5 Party (Server Hosted with card details) transactions?

Yes, the process will use the same logic as above 3 Party example. Your developer will need to calculate the SHA256 HMAC and POST the data to the Payment Server.