



Hosted Payment Page Integration Guide

Online Payment Processing for Businesses Worldwide

www.innovatepayments.com

Contents

About this guide.....	3
Copyright	3
Introduction	3
How the Hosted Payment Page works	4
Request method	5
Data Security.....	6
Timestamp	6
Signature.....	6
Optional additional information	7
Card holder name and address	7
Delivery name and address.....	8
Extra data fields	9
Return and Call-back URLs	10
Transaction Results	11
Returning to your store.....	11
Call-back fields	12
Call-back and return URL order.....	13
Transaction Advice Service	13
Hosted Payment Page Configuration	14
Activation.....	16
Uploading files	16
Verified by Visa and MasterCard SecureCode.....	18
Payment Page Extensions	19
Repeat Billing.....	19
Card Filter	19
Card Discount.....	19
Framed Payment Pages	20
Mobile Devices	21
Transparent Mode	22
Sending a transparent purchase request	23
Use within frames	24
Alternate payment methods.....	25
Response codes	26
Supported Currency Codes	28
ISO Country Codes	29
Test Cards	34
Simulating decline/error responses	34
Generating a purchase request - PHP example.....	37
Document history	39

About this guide

This guide describes how to connect your Internet shop to the Innovate Payments processing network, using our HTML integration method. To get the most from this guide, you will need to have a working knowledge of HTML, including forms.

Copyright

© 2013 Innovate Payments. All rights reserved.

While every effort has been made to ensure the accuracy of the information contained in this publication, the information is supplied without representation or warranty of any kind, is subject to change without notice and does not represent a commitment on the part of Innovate Payments. We assume no responsibility and shall have no liability, consequential or otherwise, of any kind arising from this material or any part thereof, or any supplementary materials subsequently issued by Innovate Payments. Innovate Payments has made every effort to ensure the accuracy of this material.

Introduction

This integration method allows for real-time processing of payments and ensures a maximum number of up-to-date payment methods. The Hosted Payment Page service is a secure PCI DSS compliant system, use of which does not require the merchant to have their own PCI compliance as card details are held only within the Innovate Payments systems. This is the fastest way to get up and running with on-line payments.

This integration method uses HTML messages to pass information between your site and Innovate Payments. It is the simplest and easiest method of integration and will work on just about any platform.

There is nothing to install with the Hosted Payment Page method of integration. All you need is a working Internet connection and your store ID.

How the Hosted Payment Page works

The Hosted Payment Page service allows your website with its own shopping system to work in conjunction with our payment service.

This integration method uses HTML forms to pass information to the Innovate Payments gateway for payment processing. You create the form in your web page and insert parameters that describe the purchase.

1. When a shopper is ready to pay for their goods, your website should present them with a button or link which, when selected, submits the order details to our payment page.
2. The shopper will then be taken to our payment pages to enter their payment details, such as credit/debit card details. Your website does not gather card details from the shopper - we do this in our payment pages.
3. We forward the shopper's details to the bank, where the shopper's credit worthiness is checked. The bank returns an authorised or declined response to us
4. If the payment is declined, the shopper is given two options - to try another means of payment or to cancel the purchase.
5. If the payment is completed, we then display a result page to the shopper showing the outcome of the payment transaction. We also send them a confirmation email.
6. We also inform you about the transaction. How this is done will depend upon how you have configured your options with the Merchant Interface.

All of the pages displayed by the Hosted Payment Page service can be customised to suit your website style and presentation.

Request method

All payment requests must be sent using the HTTP POST method to the Hosted Payment Page gateway URL:

`https://secure.innovatepayments.com/gateway/index.html`

The minimum information that needs to be sent is the cost and currency for the purchase, a purchase description, your store ID, and security information to ensure the data is not tampered with.

The HTML form fields that contain the basic purchase information are as follows:

Field	Description	Notes
ivp_store	Your store ID	
ivp_amount	Transaction amount	In major units, for example 9 dollars 50 cents must be sent as 9.50 not 950
ivp_currency	Currency the transaction is in	3 character ISO code
ivp_test	Test mode indicator	0 = Live, 1 = Test
ivp_timestamp	Time in seconds since Jan 1 st 1970	See the Data Security section for details.
ivp_cart	Cart ID / Order ID	Your reference for the transaction. For example, this could be a cart ID or order ID generated by your shopping system. Maximum length is 63 characters.
ivp_desc	Purchase description	Maximum length is 63 characters
ivp_extra	Which extra data blocks are present	See the Optional additional information section for details.
ivp_signature	Security check of the above data.	See the Data Security section for details.

Example request:

```
<form action="https://secure.innovatepayments.com/gateway/index.html"
      method="post">
  <input name="ivp_store" type="hidden" value="2">
  <input name="ivp_amount" type="hidden" value="19.95">
  <input name="ivp_currency" type="hidden" value="USD">
  <input name="ivp_test" type="hidden" value="1">
  <input name="ivp_timestamp" type="hidden" value="1293002624">
  <input name="ivp_cart" type="hidden" value="ABC123">
  <input name="ivp_desc" type="hidden" value="Items">
  <input name="ivp_extra" type="hidden" value="none">
  <input name="ivp_signature" type="hidden"
    value="bc8113029c18be34a673f2e28ae0c6db5bf9b734">
  <input type="submit" value="Purchase">
</form>
```

All data must be sent in UTF-8 encoding. In order to allow processing via the global card network, only certain characters can be used. These are:

Unicode set name	Characters allowed (hex code)
Basic Latin	0009, 000A, 000D, 0020-007E
Latin-1 Supplement	00A0-00FF
Latin Extended-A	0100-017F
Latin Extended-B	0180-024F

Data Security

As the purchase data is sent from your shopping system to the payment gateway via the shoppers' browser, there needs to be additional information sent to ensure that the data has not been tampered with.

Timestamp

This controls the validity of the purchase request. It is sent as the time in seconds since Jan 1st 1970, and must be generated using GMT/UTC. Using a local time zone will cause the timestamp check to fail.

If the timestamp is more than one hour old or more than 15 minutes into the future, the transaction will not be processed. This can be sent as zero to skip this check, but we advise that you include a valid timestamp if possible.

Example value:

1293002624 = Dec 22nd 2010 at 07:23:44

Signature

The signature value is generated using one of 6 hashing algorithms on the following field values:

ivp_store	ivp_amount	ivp_currency	ivp_test
ivp_timestamp	ivp_cart	ivp_desc	ivp_extra

Field values are concatenated and separated by the ':' character. They must be used in the order shown. For the example transaction shown above, this becomes:

```
2:19.95:USD:1:1293002624:ABC123:Items:none
```

A secret key is also used. The way it is used depends on the hashing algorithm selected. For non HMAC algorithms, the key must be placed before the text generated for the check, separated by a colon, for example:

```
SecretKey:2:19.95:USD:1:1293002624:ABC123:Items:none
```

If using a HMAC algorithm, then the secret key is used as the password parameter for that algorithm.

The algorithms supported are SHA1, SHA256, HMAC-SHA1 and HMAC-SHA256. MD5 and HMAC-MD5 can be enabled if required, though we strongly advise against using MD5 based algorithms.

See the Hosted Payment Page Configuration section for details on selecting the algorithm and providing your secret key. An example showing the construction of the signature as part of a purchase request using PHP is at the end of this document.

The secret key itself must never be included as part of the form details or be made available within the page source in any way (such as in a JavaScript function). The secret key must only be in server-side code, never client side.

Optional additional information

You can supply information such as the card holders name and address, and a separate delivery address if required. How this information is used depends on configuration settings you have selected.

To indicate which additional information blocks you are sending, you must set the `ivp_extra` field in the main purchase request. If an information block is not listed within the `ivp_extra` field then that block will be ignored.

If there are no additional information blocks sent as part of the request, the `ivp_extra` field must be set to the word 'none'. If one or more block is being sent, then the `ivp_extra` field must contain a comma separated list of the blocks. For example if both card holder name and address and the delivery address are sent then `ivp_extra` must be set to 'bill,delv'

Card holder name and address

Field	Description	Notes
bill_title	Title (Mr, Mrs, etc)	
bill_fname	Forenames	
bill_sname	Surname	
bill_addr1	Street address – line 1	
bill_addr2	Street address – line 2	
bill_addr3	Street address – line 3	
bill_city	City	
bill_region	Region/State	
bill_country	Country	Must be sent as a 2 character ISO code
bill_zip	Zip/Area/Postcode	
bill_email	Email address	
bill_signature	Data security check	Uses the same algorithm and key as for the main purchase details.

If sending address details, the minimum data required is: Address line 1, City and Country.

The system can be configured to allow the shopper to edit this information on the hosted payment pages, or to keep it locked. This only applies to the address information, the name and email can always be edited.

If you configure the system for locked details, then you must provide a data signature for the billing details. The signature is calculated in the same way as the main purchase details, using the same algorithm and secret key. The signature calculated for the main purchase details is used as one of the elements for generating this signature, which ensures that the billing details received are known to belong to this purchase request. The fields used in the calculation are:

bill_title	bill_fname	bill_sname	bill_addr1
bill_addr2	bill_addr3	bill_city	bill_region
bill_country	bill_zip	ivp_signature	

You must include 'bill' in the `ivp_extra` field from the main purchase request for this block to be accepted.

Delivery name and address

Field	Description	Notes
delv_title	Title (Mr, Mrs, etc)	
delv_fname	Forenames	
delv_sname	Surname	
delv_addr1	Street address – line 1	
delv_addr2	Street address – line 2	
delv_addr3	Street address – line 3	
delv_city	City	
delv_region	Region/State	
delv_country	Country	Must be sent as a 2 character ISO code
delv_zip	Zip/Area/Postcode	
delv_signature	Data security check	Uses the same algorithm and key as for the main purchase details.

If sending delivery details, the minimum data required is: Forenames, Surname, Address line 1, City and Country.

The system can be configured to allow the shopper to edit this information on the hosted payment pages, or to keep it locked.

If you configure the system for locked details, then you must provide a data signature for the delivery details. The signature is calculated in the same way as the main purchase details, using the same algorithm and secret key. The signature calculated for the main purchase details is used as one of the elements for generating this signature, which ensures that the delivery details received are known to belong to this purchase request. The fields used in the calculation are:

delv_title	delv_fname	delv_sname	delv_addr1
delv_addr2	delv_addr3	delv_city	delv_region
delv_country	delv_zip	ivp_signature	

You must include 'delv' in the `ivp_extra` field from the main purchase request for this block to be accepted.

Extra data fields

Field	Description	Notes
xtra_<name>	Extra data field(s)	Name must be between 1 and 15 characters long. Must only consist of lower-case letters, digits or the underscore character.
xtra_fields	Data field list	A comma separated list of all of the xtra_ elements, not including xtra_fields or xtra_signature
xtra_signature	Data security check	Uses the same algorithm and key as for the main purchase details.

These optional extra data fields can be used to hold additional data that relates to this transaction.

An example use of these is to record unique customer information such as an account ID within your system.

You can include a number of extra data fields, but the name for each field must be unique. A list of the extra data fields must be sent as 'xtra_fields'. This is to ensure that no other extra data fields get added to the request.

The signature is calculated in the same way as the main purchase details, using the same algorithm and secret key. The signature calculated for the main purchase details is used as one of the elements for generating this signature, which ensures that the extra data details received are known to belong to this purchase request. The fields used in the calculation are:

xtra_<name> xtra_fields ivp_signature

For example, if you are sending two extra data fields named as 'xtra_account' and 'xtra_section' then you need to set xtra_fields as follows:

xtra_fields = xtra_account,xtra_section

This would result in the signature being calculated from:

xtra_account xtra_section xtra_fields ivp_signature

The order of the extra data fields in the signature calculation must be the same as the order in which they are listed within xtra_fields.

You must include 'xtra' in the ivp_extra field from the main purchase request for this block to be accepted.

Return and Call-back URLs

Field	Description	Notes
return_auth	Return after authorisation	These control the URL used to return the customer to your store.
return_decl	Return after declined	
return_can	Return after cancellation	
return_cb_auth	Call-back for authorisation	These control the URLs used by the call-back system to update your store with the transaction results.
return_cb_decl	Call-back for declined	
return_cb_can	Call-back for cancelled	
return_signature	Data security check	Uses the same algorithm and key as for the main purchase details.

These can be used to override the URL's set as part of the payment page configuration.

Please see the section below (Transaction Results) for details regarding the use of return and call-back URLs.

All URL's must be fully qualified. For a value to be accepted as a valid URL, it must start either http: or https:

You can also use the value 'none' to indicate that no action should be taken at that point, or 'default' to indicate that the pre-configured value should be used. If the URL is not valid, then the pre-configured URL will be used.

IMPORTANT NOTE: Call-back URL's are used directly as a server-to-server connection, they do not operate via the customers browser. As such, they must be URL's which can be accessed over the public internet. Private URL's or IP addresses must not be used. Only connections to port 80 or 443 can be made. The Call-back URL must return with a HTTP status code of '200 OK'. Other status codes will be taken to mean that the request did not complete as expected.

For the return URL's you can prefix the address with 'auto:' to indicate that the return should happen automatically, i.e. not requiring the customer to click on any buttons or links for this to happen. This will only work if the customer has JavaScript enabled in their browser.

auto:http://www.storename.com/

The signature is calculated in the same way as the main purchase details, using the same algorithm and secret key. The signature calculated for the main purchase details is used as one of the elements for generating this signature, which ensures that the URL details received are known to belong to this purchase request. The fields used in the calculation are:

return_cb_auth	return_cb_decl	return_cb_can	return_auth
return_decl	return_can	ivp_signature	

You must include 'return' in the ivp_extra field from the main purchase request for this block to be accepted.

Transaction Results

In order for your system to be updated with the result of the transaction you can configure three different call-back addresses. These are URL's which will be called directly by the Innovate Payments gateway and will contain details of the transaction and its status. The details will be sent using the HTTP POST method. A different URL can be defined for each of the following events:

Transaction Authorised
Transaction Declined
Transaction Cancelled

You can use the same URL for each event, in which case you will need to examine the `auth_status` field to determine if the call-back is for an authorised transaction or not. See the table on the next page for a complete list of fields.

You could get more than one call-back for the same transaction as the system allows for the shopper to re-try should the transaction be declined.

The call-back data, which is sent using the HTTP POST method, can be authenticated using the same signature method as used in the request. The field `auth_hash` will contain a signature consisting of the following fields:

<code>auth_status</code>	<code>auth_code</code>	<code>auth_message</code>	<code>auth_tranref</code>
<code>auth_cvv</code>	<code>auth_avs</code>	<code>card_code</code>	<code>card_desc</code>
<code>cart_id</code>	<code>cart_desc</code>	<code>cart_currency</code>	<code>cart_amount</code>
<code>tran_currency</code>	<code>tran_amount</code>	<code>tran_cust_ip</code>	

`bill_hash` will contain a signature consisting of the following fields:

<code>bill_title</code>	<code>bill_fname</code>	<code>bill_sname</code>	<code>bill_addr1</code>
<code>bill_addr2</code>	<code>bill_addr3</code>	<code>bill_city</code>	<code>bill_region</code>
<code>bill_country</code>	<code>bill_zip</code>	<code>bill_phone1</code>	<code>bill_email</code>
<code>auth_hash</code>			

`delv_hash` will contain a signature consisting of the following fields:

<code>delv_title</code>	<code>delv_fname</code>	<code>delv_sname</code>	<code>delv_addr1</code>
<code>delv_addr2</code>	<code>delv_addr3</code>	<code>delv_city</code>	<code>delv_region</code>
<code>delv_country</code>	<code>delv_zip</code>	<code>delv_phone1</code>	<code>auth_hash</code>

Returning to your store

Once the shopper has either authorised or cancelled the transaction, they can be returned to your store. You should not rely on this happening as the shopper could close their browser before following the link back. You can define a different URL for authorised, declined and cancelled transactions. These must not be used to update your system with the result of the transaction; instead you should use the call-back options for that.

Call-back fields

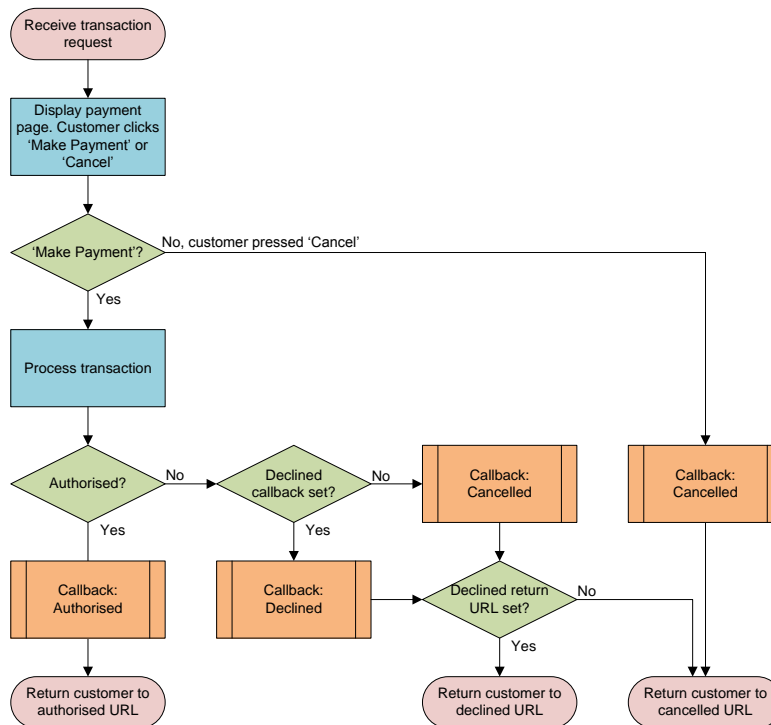
The call-back fields are sent using the HTTP POST method.

Field	Description	Notes
auth_status	Authorisation result	'A' or 'H' indicate an authorised transaction. Any other value indicates that the request could not be processed.
auth_code	Authorisation code	If the transaction was authorised, this contains the authorisation code from the acquirer. Otherwise it contains an error code. See the response codes section for more details.
auth_message	Authorisation message	
auth_tranref	Transaction reference	Allocated by Innovate Payments gateway
auth_cvv	Result of the CVV check	Y = CVV matched OK N = CVV not matched X = CVV not checked E = Error, unable to check CVV
auth_avs	Result of the AVS check	Y = AVS matched OK N = AVS not matched X = AVS not checked E = Error, unable to check AVS P = Partial match (for example, post-code only)
card_code	2 character card type	
card_desc	Card description	e.g. 'Visa Credit ending 0002'
cart_id	Cart ID	Copied from the purchase request
cart_desc	Purchase description	Copied from the purchase request
cart_currency	Requested currency	The transaction currency and amount may be different from the requested values if you have a multi-currency store and the shopper changes the currency.
cart_amount	Requested amount	
tran_currency	Transaction currency	
tran_amount	Transaction amount	
tran_cust_ip	Customer IP Address	
auth_hash	Data signature	Signature of the auth, card, cart and tran fields
bill_title	Title (Mr, Mrs, etc)	
bill_fname	Forenames	
bill_sname	Surname	
bill_addr1	Street address – line 1	
bill_addr2	Street address – line 2	
bill_addr3	Street address – line 3	
bill_city	City	
bill_region	Region/State	
bill_country	Country	2 character ISO code
bill_zip	Zip/Area/Postcode	
bill_phone1	Phone number	
bill_email	Email address	
bill_hash	Data signature	Signature of the bill fields and auth_hash
delv_title	Title (Mr, Mrs, etc)	
delv_fname	Forenames	
delv_sname	Surname	
delv_addr1	Street address – line 1	
delv_addr2	Street address – line 2	
delv_addr3	Street address – line 3	
delv_city	City	
delv_region	Region/State	
delv_country	Country	2 character ISO code
delv_zip	Zip/Area/Postcode	
delv_phone1	Phone number	
delv_hash	Data signature	Signature of the delv_fields and auth_hash
xtra_<name>	Extra data fields	Copied from the purchase request

Call-back and return URL order

If a call-back URL is defined, then a direct server-to-server connection will be made to that URL as soon as the authorisation results have been obtained. The payment page will still show the Transaction Processing page whilst waiting for the call-back to complete; as such you should ensure that the system handling the call-back is able to do so quickly.

Once the call-back has been completed, the payment pages will display the transaction results page, which includes the link allowing the customer to return to your store.



Transaction Advice Service

The transaction advice service is similar in operation to the Call-back system. The key differences between the two methods are that the Call-back system is part of the hosted payment page authorisation process, and as such only relates to the initial authorisation request. The Transaction advice service can be used to send details of events such as refunds or voids that are processed through the Merchant Administration System in addition to the initial authorisation request.

For see the Transaction Advice Service integration guide for more details.

Hosted Payment Page Configuration

The Payment Page section of the merchant administration system allows you to set the various options such as call-back URLs and security check methods. You can also configure the colours, fonts and images used on the payment page. There are options for uploading your own images and HTML to use within the page.

The first screen covers the call-back and return URL's, display of delivery and billing address information and the security data. If the delivery or billing address details are locked, then they must be provided as additional data with the purchase request. The sections covered by this screen are:

- | | |
|------------------------------|-----------------------------------|
| Delivery and billing details | - Optional additional information |
| Signature values | - Data Security |
| Call-back and return URL's | - Transaction Results |

Payment page configuration

Purchase form		
Show store name	<input type="text" value="No"/>	Display your store name below the purchase description
Disable delivery section	<input type="text" value="Yes"/>	If this is disabled then the payment form will not have a section allowing the user to enter any delivery details.
Lock delivery details	<input type="text" value="No"/>	This allows you to lock the delivery details supplied within the request. The consumer cannot change the details, and no delivery section will be displayed. If you select this option then you must provide delivery details with the request or the request will be rejected.
Lock billing address	<input type="text" value="No"/>	This allows you to lock the billing address details supplied within the request. The consumer cannot change the billing details, and no billing address section will be displayed. If you select this option then you must provide billing details with the request or the request will be rejected. NOTE: The consumer can still change the name and email address used, but not the postal address.
Contact number	<input type="text" value="Yes - Optional"/>	This controls if a contact telephone number field appears within the billing section. If this is set as mandatory, and the lock billing address is also set then the telephone number must be supplied as part of the purchase request.
Allow Arabic input	<input type="text" value="No"/>	Enable this if you wish to accept Arabic text in the name or address parts of the payment pages.
Card only mode	<input type="text" value="No"/>	If this is enabled, then no billing or card holder sections will be displayed. All required billing details and card holder details (including forename, surname and email) must be supplied as part of the transaction request.
Transaction mode		
Automatic capture	<input type="text" value="Yes"/>	If automatic capture is disabled, you will need to manually capture each authorised transaction in order to complete payment. This is sometimes known as pre-authorisation mode.
Data security		
Data integrity hash type	<input type="text" value="SHA1"/>	Which algorithm is used to generate the data signature. This ensures that the data cannot be tampered with. We would recommend using a HMAC algorithm if possible.
Data integrity secret key	<input type="text"/>	The secret key used when generating the data signature. You must ensure that this is not disclosed in any way.
Data signature checks		
Some optional data sections (additional information sent as part of the transaction request) can have their signature checks skipped. If a signature check is skipped, then the system will not be able to determine if any of the data for that section has been tampered with.		
Skip billing signature	<input type="text" value="No"/>	If set to yes, then the billing signature will not be checked.
Skip delivery signature	<input type="text" value="No"/>	If set to yes, then the delivery signature will not be checked.
Transaction callback		
The gateway can make a connection back to your server to update it with the result of any transaction. This callback is made directly from the gateway to your server, it does not go via the consumers' browser.		
Authorised	<input type="text"/>	
Declined	<input type="text"/>	
Cancelled	<input type="text"/>	
Void if callback fails	<input type="text" value="No"/>	For authorised transactions, if the callback fails you can select to have the transaction voided. The cardholder will not be charged, and will see a declined result.
Return URL		
Here you must define the URL that the consumer will be directed to upon completion of the transaction. If the declined URL is not set, then the cancelled URL will be used instead. NOTE: You should not rely on either of these being followed as the consumer could close their browser before clicking on the button to return to your site. You should use the callback options above to ensure that you are updated with the result of any transaction.		
Authorised	<input type="text"/>	
Declined	<input type="text"/>	
Cancelled	<input type="text"/>	

NOTE: Any changes made will only affect the test mode settings. You must use the Activation process described later in this document to copy these settings to the live mode system.

Colours, fonts and page background image.

You can specify what colours are used within the payment page, allowing you to change them to colours which match your own site. The page displayed to the shopper is built up from several sections; you can supply the HTML content for 4 of these sections (see the Additional Files section of this document).

The page is built using a centralised section for the user to enter their details. This section can be displayed in various different layouts, and is known as the 'Form area'. Within this form area there is the actual payment form, the colours for this are set in the 'Table area' and 'Input fields' part of the customisation screen.

Payment page customisation

Page				
Background colour	<input type="text" value="FFFFFF"/>			
Default font size	<input type="text" value="12"/>	(Pixels. Min 8, Max 20)		
Background image	<input type="text" value="None"/>			
Stretch to fit page	<input type="text" value="No"/>			
Image repeat	<input type="text" value="No"/>			
Image position	<input type="text" value="Top"/>	<input type="text" value="Left"/>		
Form area				
Background colour	<input type="text" value="FFFFFF"/> (Enter 'None' to make the background transparent)			
Text colour	<input type="text" value="000000"/>			
Logo	<input type="text" value="None"/> (This logo will be placed above the payment form)			
Logo position	<input type="text" value="Right"/>			
Layout				
Layout size	<input type="text"/>	(Min page width)	<input type="text"/>	(Section width)
	<input type="text"/>	(Form width)		
Field size	<input type="text"/>	(Icon column)	<input type="text"/>	(Prompt column)
	<input type="text"/>	(Input field size)	<input type="button" value="Set Defaults"/>	
Card logos				
Logo set	<input type="text" value="1"/> (Preview)			
Include 3D Secure logos	<input type="text" value="Yes"/> (E.g. Verified by Visa. Not all sets contain these, but it is recommended to display them when available)			
Table area				
Background colour	<input type="text" value="DBEDF5"/> (Enter 'None' to make the background transparent)			
Text colour	<input type="text" value="000000"/>			
Border size	<input type="text" value="0"/> (Pixels. 0 to indicate no border)			
Border colours	<input type="text" value="000000"/> (Top)	<input type="text" value="000000"/> (Right)	<input type="text" value="000000"/> (Bottom)	<input type="text" value="000000"/> (Left)
Headers				
Header background colour	<input type="text" value="3D4043"/>			
Header text colour	<input type="text" value="FFFFFF"/>			
Header font size	<input type="text" value="14"/> (Pixels. Min 8, Max 20)			
Input fields				
Background colours	<input type="text" value="F8F8FC"/> (Standard)	<input type="text" value="D78BA5"/> (Error highlight)		
Border colours	<input type="text" value="C3C5CC"/> (Top)	<input type="text" value="929499"/> (Right)	<input type="text" value="929499"/> (Bottom)	<input type="text" value="C3C5CC"/> (Left)
Note text colour	<input type="text" value="000000"/>			
Note font size	<input type="text" value="10"/> (Pixels. Min 8, Max 20)			
Links				
Colour	<input type="text" value="0F5173"/>			
Colour when mouse over	<input type="text" value="000000"/>			

Countries

You can choose to limit which countries are displayed in the billing address and delivery address sections of the payment page. The countries are shown as a drop-down selection, which normally includes all countries.

Activation

Any changes you make to the payment page configuration, including the upload of additional files, only affects the test mode version of your payment page. You can make changes at any time without affecting the live transaction processing. Once you have completed the changes and want to update the live processing system to reflect these changes, you need to go to the Activation page.

Here you can choose to copy all of the test mode settings across to the live system.

If you have made changes to the test system that you are not happy with, there is the choice to copy the current live settings back to the test system.

Activation

Activate

This will take the current configuration settings for the test mode transactions and copy them over to the live system. Any changes that you have made to the payment page will then be visible to your customers.

WARNING: This can not be undone. You must tick the confirm box before clicking on the button.

☐ Confirm

Activate

Restore

This will take the current configuration settings from the live payment pages and copy them into the test mode system. Any changes that you may have made to the test settings will be lost.

WARNING: This can not be undone. You must tick the confirm box before clicking on the button.

☐ Confirm

Restore

Uploading files

Images

You can upload image files in gif or jpg format for use within the payment page customisation. These can be selected for use as background images or logos, or they can be referenced by HTML files that you upload. The maximum size of an image file is 256K.

HTML Files

There are seven HTML files that can be uploaded. These files are not complete HTML pages; they should be treated as HTML fragments that are included within other pages.

The first four of these files are used within the main payment page, which is constructed as follows:

Page header. Content can be set by uploading a file called ' page_header.html '. This section is the full width of the page.		
	Form header. Content can be set by uploading a file called ' form_header.html '	
	Form logos. Generated by the Innovate Payments gateway.	
	Payment form. Generated by the Innovate Payments gateway.	
	Card logos. Generated by the Innovate Payments gateway.	
	Form trailer. Content can be set by uploading a file called ' form_trailer.html '	
Page trailer. Content can be set by uploading a file called ' page_trailer.html '. This section is the full width of the page.		

The remaining three files can be used to add additional text to the payment completed, payment failed or payment cancelled pages. The list of files that can be uploaded is as follows:

Filename	Used in
page_header.html	Displayed at the top of the payment page
form_header.html	Displayed above the data entry form
form_trailer.html	Displayed below the data entry form
page_trailer.html	Displayed at the bottom of the payment page
auth_thanks.html	Displayed within the transaction completed page once an authorisation has been obtained.
auth_failed.html	Displayed within the transaction failed page. This page gives the consumer the option to try again with another card, or to cancel the transaction.
auth_cancel.html	Displayed within the transaction cancelled page.

See the section on Mobile Devices for alternate filenames that are used when displaying the payment page on systems such as smart phones.

The HTML files uploaded must be treated as HTML fragments, not as complete documents. As such they must not contain tags such as <html>, <head> or <body>. The files must not include any JavaScript, forms, frames or objects. If they reference objects such as images then those must be sourced from a secure (https) server. The best option is to upload those images to the Innovate Payments gateway. To reference an image uploaded to the gateway use the sequence `{{FileBase}}` to have the correct URL inserted at that point - the URL will change depending on if the page is viewed in test or live mode.


For example, to reference an image uploaded as logo.gif you should use the following:

```

```

Verified by Visa and MasterCard SecureCode

After the consumer enters their card details, the Innovate Payments gateway will check to see if that card is enrolled as part of the Verified by Visa or MasterCard SecureCode authentication systems. Whilst this check is done, a page will be displayed advising the consumer that the next page they see may be a from their card issuer.




Please wait while your transaction is processed.

■■■■■■■■■■ The next screen you see may be payment card verification through your card issuer.

Do not click the refresh or back button or your transaction may be interrupted.

Powered by Innovate Payments | [Website Terms & Conditions](#) | [Privacy policy](#)

If the card is part of one of these authentication systems, then an additional page is displayed which requires the relevant authentication details to be entered. This is usually in the form of a password that has been assigned by the consumer. The actual data entry section is presented directly by the card issuer and cannot be customised. The form is displayed as an inline frame within the payment pages, allowing the remainder of the page to retain the customisation that has been defined, which helps to reassure the consumer that it is part of the payment process. If the two column layout has been selected, then an information section will appear next to the form showing the consumer details of the purchase they are making.



Cardholder Verification

Verified by Visa and MasterCard SecureCode

Please enter your details into the form opposite. This form comes directly from your card issuer.

Your transaction details are as follows:

Description:	Sample Item
From:	Innovate Payments
Cost:	Dh399.00

Verified by VISA

Added Protection

Please submit your Verified by Visa password

Merchant: Innovate Payments

Amount: 399.00

Date: 01/03/2011

Card number: **** * 0002

Password:

[Forgot your password?](#)

Do not click the refresh or back button or your transaction may be interrupted.

Powered by Innovate Payments | [Website Terms & Conditions](#) | [Privacy policy](#)

The data entry section is usually presented by the card issuers on a white background. You cannot alter the colours or images used in this part. The frame section will use the same border colours as have been defined for the payment form input fields.

Payment Page Extensions

Extensions modules are available which can be used to add additional options to a transaction request. Details of the available extensions are held in a separate guide, titled Payment Page Extensions.

Extensions available are:

Repeat Billing

The Repeat Billing system gives merchants who use the Innovate Payments Hosted Payment Pages the ability to setup and manage recurring payments, such as those used in a subscription service.

Card Filter

This module allows you to send details of pre-registered card numbers as part of the transaction request.

This could be used, for example, by a service provider who first requires a customer to visit their premises and register in person in order to use their systems.

Card Discount

This module allows you to offer a discount depending upon the card that was used to complete the transactions.

Framed Payment Pages

The Hosted Payment Pages can be used within a frame if required, which allows them to be used whilst retaining your domain details within the browser navigation bar.

NOTE: In order to use the framed option, you must first contact our support team and request that it is enabled for your account. Your site must be operating on a secure (https) server in order for the framed option to be considered. Even though the Hosted Payment Pages are on a secure (https) server, the browser will not display its usual secure page indicator, often a padlock or other indicator in the URL display, unless the top level page is also a secure server.

To use the framed option, you must submit the purchase data to `/gateway/framed.html` instead of `/gateway/index.html`

```
https://secure.innovatepayments.com/gateway/framed.html
```

This could be done from within the framed area itself, or from outside of the frame as long as the form target contains the name of the framed area.

The required size of the frame will depend upon the payment page layout in use. The two column layout will require a minimum frame width of 1000 pixels. The single column layout will require a minimum frame width of 600 pixels. The frame height should be a minimum of 550 pixels to allow the 3D Secure (Verified by Visa and MasterCard SecureCode) authentication pages.

The final return from the hosted payment pages back to your system (using the return URLs defined in the payment page configuration) will be within the framed area.

Mobile Devices

The Hosted Payment Pages support mobile devices, through the use of a layout that is optimised for a narrow display. The Innovate Payments server will automatically use the mobile layout if the transaction request comes through a browser that is identified as a mobile device.

You can choose to force the use of the mobile layout or the standard layout by using an alternate URL when sending the purchase request:

Transaction URL	Use mobile layout
https://secure.innovatepayments.com/gateway/index.html	Auto-detect
https://secure.innovatepayments.com/gateway/mobile.html	Yes
https://secure.innovatepayments.com/gateway/standard.html	No

For users that are browsing using a tablet device, the standard page layout is generally the preferred option.

When operating in mobile mode, the payment page uses the same customisation and configuration options as used in standard mode, but will use a different set of additional html files. This allows you to upload page headers/trailers that are designed specifically for mobile devices.

HTML file name in standard mode	HTML file name in mobile mode
page_header.html	page_header_mob.html
form_header.html	form_header_mob.html
form_trailer.html	form_trailer_mob.html
page_trailer.html	page_trailer_mob.html

Transparent Mode

Transparent Mode allows the merchant to use the Innovate Payments gateway without displaying the payment pages. This requires the merchant to collect all of the payment details, including the card number, expiry date and card security code, on the merchants own system.

As the merchant is responsible for collecting the card details, the merchant must be operating on a secure (https) server, and must be certified PCI DSS compliant.

Using this method, the Innovate Payments servers will not actually display any payment pages. The transaction details received are processed and the results returned back to the merchant system. It is up to the merchant system to display the appropriate results page.

Should the payment require additional authentication, for example a 3-D Secure system such as Verified by Visa or MasterCard SecureCode, then this method will automatically redirect the customers' browser to the appropriate authentication pages before continuing with the transaction.

You will need to request that transparent mode is enabled for your account; this is not enabled by default.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a global Card Scheme initiative that aims to ensure that every entity that handles, stores or processes cardholder data does so in a secure manner. MasterCard and Visa have combined their own security standards for cardholder data creating an aligned program, which is now endorsed by American Express, JCB and Diners. Much of PCI DSS relates to the technology involved in capturing and processing card data and this is particularly relevant to those merchants who process and capture cardholder data on their own systems rather than those who use the secure Innovate Payments hosted payment pages.

For more information, please refer to PCI DSS and to the PCI Security Standards Council at: www.pcisecuritystandards.org. If you want any help to gain compliance this site also lists PCI approved Quality Security Assessors (QSA's) who can provide technical advice.

Sending a transparent purchase request

This is done in the same way as sending a normal purchase request to the Hosted Payment Pages. As a minimum, this must include the basic transaction details and all of the details required for the customer billing address (the 'bill' extra section).

In addition to the fields required for these two sections, there are four other parameters required:

Field	Description	Mandatory
ivp_cn	Card number	Yes
ivp_exm	Card expiry date – month (numeric value 1..12)	Yes
ivp_exy	Card expiry date – year (numeric value, 4 digit year)	Yes
ivp_cv	Card security code (CVV)	Yes

These parameters do not form part of the transaction data signature.

Instead of posting the request to the standard URL, the details must instead be sent to:

`https://secure.innovatepayments.com/gateway/trans.html`

Transaction Results

The standard call-back system is used, though it differs slightly in that there is no option to retry a transaction should it fail. If that is required, then it must be implemented within the merchant systems.

You should set the declined and cancelled call-back details to the same value. The authorised call-back URL can be different if required.

As with the standard system, you must not rely on the return URL being followed to complete the transaction, or as a way of confirming the transaction status. You must use the call-back system to track the transaction status.

In the event that the transaction cannot be processed, the return URL used will be the transaction cancelled URL. All URL's (call-back and return) must be to secure URLs, i.e. they must start https://

URL's that do not start https:// will be ignored and the system will act as if no URL has been set.

Activity indicators

You should display something to the cardholder that lets them know authorisation is in progress. It may take several seconds for the initial cardholder authentication enrolment checks to be undertaken, and for the authorisation process to be completed. You don't want the cardholder to think that the process has stopped and abort the purchase.

The activity indicators should include some visual movement to reassure the cardholder that the process is continuing.

Use within frames

Transparent mode can be used within a frame if required. As the payment process may include an additional authentication step (such as Verified by Visa or MasterCard SecureCode) the frame must be a minimum of 390x400 pixels in size to allow for the display of the 3-D Secure pages.

Alternate payment methods

In addition to being able to pay using a credit/debit card, it is possible to offer PayPal as a payment method within the Hosted Payment Pages. For more information, please see the Innovate Payments PayPal integration guide, which can be downloaded from the guides section of the Merchant Administration System.









Purchase details

Description: Example
Cost: Dh50.00

Select payment method

☒ Card
☐ PayPal



Card details

* Card number:

* Expiry date:

* Security code: [What is this?](#)

Cardholder details

Title: *E.g. Mr, Mrs etc.*

* Forenames:

* Surname:

* Address line 1:

Address line 2:

Address line 3:

* City/Suburb:

Region/State:

* Country:

Post/Area code:

* Email address:

Powered by Innovate Payments | [Website Terms & Conditions](#) | [Privacy policy](#)

Response codes

Status	Code	Message
A	<i>Set by issuer</i>	Authorised
H	<i>Set by issuer</i>	Authorised, but placed on hold. Manual inspection required
E	01	Invalid request
E	02	Transaction cost or currency not supplied
E	03	Cart ID not set
E	04	Invalid store ID
E	05	Transaction cost or currency not valid
E	06	Invalid transaction mode
E	07	Card expiry not supplied
E	10	Card number not supplied
E	11	Invalid card number
E	12	Card expired
E	14	Card type mismatch
E	15	Invalid card security code
E	16	Card security code not supplied
E	17	Name not valid/not supplied
E	18	Address not valid/not supplied
E	19	Country not valid/not supplied
E	20	IP address not valid/not supplied
E	21	Card/Currency combination not supported
E	22	Invalid transaction reference
E	23	Amount differs from original
E	24	Currency differs from original
E	25	Original transaction not authorized
E	26	Original transaction already voided
E	27	Original transaction not a sale
E	28	Original transaction not a refund
E	29	Amount greater than available balance
E	30	Card details differ from original
D	31	Not authorized
D	32	Original transaction cannot be voided
C	33	Transaction cancelled
D	34	No response
E	35	Unable to refund
E	36	Previous transaction is on hold
D	37	Blocked by acquirer
E	38	Invalid expiry date
E	39	Invalid transaction class
E	40	Invalid transaction type
D	41	Insufficient funds
D	42	Card security code mismatch
E	43	Email not valid/not supplied
E	44	Phone number not valid/not supplied
E	45	Transaction mode differs from original
D	46	3DSecure authentication not available for this card
D	47	3DSecure authentication rejected

Status	Code	Message
E	48	Description not set
D	49	Sold out
E	50	Card is for ATM use only
D	51	Transaction part 1 not authorised
D	52	Transaction part 2 not authorised
X	53	Authorisation expired
E	54	Transaction part not specified
E	55	Unable to access transaction part
E	56	Duplicate transaction
D	57	Continuous authority not available on referenced transaction
E	58	Error connecting to PayPal
D	80	Not authorised <i>Card Filter module. Message text can be changed.</i>
D	90	Not authorised
D	91	Not authorised
D	92	Not authorised
E	98	Internal system error
E	99	Unknown error

Supported Currency Codes

AED	United Arab Emirates Dirham
BHD	Bahraini Dinar
CAD	Canadian Dollar
EUR	Euro
IDR	Indonesian Rupiah
GBP	Pound Sterling
JPY	Japanese Yen
KHR	Cambodian Riel
KWD	Kuwaiti Dinar
MYR	Malaysian Ringgit
OMR	Omani Rial
PHP	Philippine Peso
QAR	Qatari Rial
SAR	Saudi Riyal
SGD	Singapore Dollar
THB	Thai Baht
USD	US Dollar
VND	Vietnamese Dong

ISO Country Codes

AF	Afghanistan
AL	Albania
DZ	Algeria
AS	American Samoa
AD	Andorra
AO	Angola
AI	Anguilla
AG	Antigua and Barbuda
AR	Argentina
AM	Armenia
AW	Aruba
AU	Australia
AT	Austria
AZ	Azerbaijan
BS	Bahamas
BH	Bahrain
BD	Bangladesh
BB	Barbados
BY	Belarus
BE	Belgium
BZ	Belize
BJ	Benin
BM	Bermuda
BT	Bhutan
BO	Bolivia
BA	Bosnia and Herzegovina
BW	Botswana
BR	Brazil
IO	British Indian Ocean Territory
VG	British Virgin Islands
BN	Brunei Darussalam
BG	Bulgaria
BF	Burkina Faso
BI	Burundi
KH	Cambodia
CM	Cameroon
CA	Canada
CV	Cape Verde
KY	Cayman Islands
CF	Central African Rep
TD	Chad
CL	Chile
CN	China
CX	Christmas Island
CC	Cocos (Keeling) Islands
CO	Colombia
KM	Comoros

CD	Congo, Democratic Rep of
CG	Congo, Republic of
CK	Cook Islands
CR	Costa Rica
CI	Cote d'Ivoire
HR	Croatia
CU	Cuba
CY	Cyprus
CZ	Czech Rep
DK	Denmark
DJ	Djibouti
DM	Dominica
DO	Dominican Rep
EC	Ecuador
EG	Egypt
SV	El Salvador
GQ	Equatorial Guinea
ER	Eritrea
EE	Estonia
ET	Ethiopia
FK	Falkland Islands
FO	Faroe Islands
FJ	Fiji
FI	Finland
FR	France
GF	French Guyana
PF	French Polynesia
GA	Gabon
GM	Gambia
GE	Georgia
DE	Germany
GH	Ghana
GI	Gibraltar
GR	Greece
GL	Greenland
GD	Grenada
GP	Guadeloupe
GU	Guam
GT	Guatemala
GN	Guinea
GW	Guinea-Bissau
GY	Guyana
HT	Haiti
HN	Honduras
HK	Hong Kong
HU	Hungary
IS	Iceland
IN	India
ID	Indonesia
IR	Iran

IQ	Iraq
IE	Ireland
IT	Italy
JM	Jamaica
JP	Japan
JO	Jordan
KZ	Kazakhstan
KE	Kenya
KI	Kiribati
KP	Korea, North
KR	Korea, South
KW	Kuwait
KG	Kyrgyzstan
LA	Laos
LV	Latvia
LB	Lebanon
LS	Lesotho
LR	Liberia
LY	Libya
LI	Liechtenstein
LT	Lithuania
LU	Luxembourg
MO	Macau
MK	Macedonia
MG	Madagascar
MW	Malawi
MY	Malaysia
MV	Maldives
ML	Mali
MT	Malta
MH	Marshall Islands
MQ	Martinique
MR	Mauritania
MU	Mauritius
YT	Mayotte
MX	Mexico
FM	Micronesia
MD	Moldova, Rep of
MC	Monaco
MN	Mongolia
ME	Montenegro
MS	Montserrat
MA	Morocco
MZ	Mozambique
MM	Myanmar
NA	Namibia
NR	Nauru
NP	Nepal
NL	Netherlands
AN	Netherlands Antilles

NC	New Caledonia
NZ	New Zealand
NI	Nicaragua
NE	Niger
NG	Nigeria
NU	Niue
NF	Norfolk Island
MP	Northern Mariana Islands
NO	Norway
OM	Oman
PK	Pakistan
PW	Palau
PS	Palestinian Territory, Occupied
PA	Panama
PG	Papua New Guinea
PY	Paraguay
PE	Peru
PH	Philippines
PN	Pitcairn Islands
PL	Poland
PT	Portugal
PR	Puerto Rico
QA	Qatar
RE	Reunion
RO	Romania
RU	Russian Federation
RW	Rwanda
WS	Samoa
SM	San Marino
ST	Sao Tome and Principe
SA	Saudi Arabia
SN	Senegal
RS	Serbia
SC	Seychelles
SL	Sierra Leone
SG	Singapore
SK	Slovakia
SI	Slovenia
SB	Solomon Islands
SO	Somalia
ZA	South Africa
ES	Spain
LK	Sri Lanka
SH	St Helena
KN	St Kitts and Nevis
LC	St Lucia
PM	St Pierre and Miquelon
VC	St Vincent and Grenadines
SD	Sudan
SR	Suriname

SZ	Swaziland
SE	Sweden
CH	Switzerland
SY	Syria
TJ	Tajikistan
TW	Taiwan, Rep of China
TZ	Tanzania
TH	Thailand
TL	Timor-Leste
TG	Togo
TK	Tokelau
TO	Tonga
TT	Trinidad and Tobago
TN	Tunisia
TR	Turkey
TM	Turkmenistan
TC	Turks and Caicos Islands
TV	Tuvalu
UG	Uganda
UA	Ukraine
AE	United Arab Emirates
GB	United Kingdom
VI	United States Virgin Islands
US	United States of America
UY	Uruguay
UZ	Uzbekistan
VU	Vanuatu
VA	Vatican City
VE	Venezuela
VN	Viet Nam
WF	Wallis and Futuna Islands
EH	Western Sahara
YE	Yemen
ZM	Zambia
ZW	Zimbabwe

Test Cards

These card numbers can be used when testing your integration to Innovate Payments. These cards will not work for live transactions.

Card number	Type	CVV	MPI
4000 0000 0000 0002	Visa	123	No
4111 1111 1111 1111	Visa	123	Yes
4444 3333 2222 1111	Visa	123	Yes
4444 4244 4444 4440	Visa	123	Yes
4444 4444 4444 4448	Visa	123	Yes
4012 8888 8888 1881	Visa	123	Yes
5105 1051 0510 5100	Mastercard	123	No
5454 5454 5454 5454	Mastercard	123	Yes
5555 5555 5555 4444	Mastercard	123	Yes
5555 5555 5555 5557	Mastercard	123	Yes
5581 5822 2222 2229	Mastercard	123	Yes
5641 8209 0009 7002	Maestro UK	123	Yes
6767 0957 4000 0005	Solo	123	No
3434 343434 34343	American Express	1234	No
3566 0020 2014 0006	JCB	123	No

The card security code (CVV) to use with the test cards is 123 (except for American Express, which should be 1234) for an authorised response, other codes will be declined.

Cards which show 'Yes' in the MPI column will use a simulated 3D Secure authentication page, allowing you to test the transaction flow when Verified by Visa or MasterCard SecureCode is used.

Simulating decline/error responses

When in test mode, and when using the above test cards, you can simulate any of the transaction alternate payment methods

in addition to being able to pay using a credit/debit card, it is possible to offer paypal as a payment method within the hosted payment pages. for more information, please see the innovate payments paypal integration guide, which can be downloaded from the guides section of the merchant administration system.

**Purchase details**

Description: Example
Cost: Dh50.00

Select payment method☒ Card☐ PayPal**Card details**

* Card number:
* Expiry date: --Month-- --Year--
* Security code: [What is this?](#)

Cardholder details

Title: *E.g. Mr, Mrs etc.*
* Forenames: Test
* Surname: Customer
* Address line 1: Address
Address line 2:
Address line 3:
* City/Suburb: City
Region/State: Dubai
* Country: United Arab Emirates
Post/Area code: abc123
* Email address: test@test.com

Powered by Innovate Payments | [Website Terms & Conditions](#) | [Privacy policy](#)

response codes by using specific values for the card security code (CVV). By taking the response code you want to simulate, pad that code with a leading '0' in order to make it a 3 digit code and use that for the CVV.

For example, to simulate the Insufficient Funds response (status 'D', code '41') use 041 as the CVV.

You can also simulate an on-hold transaction in the same way. On hold is where the transaction has been authorised, but the anti-fraud system has flagged the transaction for inspection. Whilst the transaction is on-hold, no funds will be debited from the customers' card. You would need to use the Merchant Administration System to either accept or reject the transaction. To simulate the on-hold response within the test system, use a CVV value of '999' with one of the above test cards.

Generating a purchase request - PHP example

This is an example of creating a purchase request that is signed using the SHA1 algorithm.

Notes regarding this example are on the following page.

```
<html><head><title>Purchase Example</title></head>
<body>
<form action="https://secure.innovatepayments.com/gateway/index.html" method="post">
<?php
function SignData($post_data,$secretKey,$fieldList) {
    $signatureParams = explode(',', $fieldList);
    $signatureString = $secretKey;
    foreach ($signatureParams as $param) {
        if (array_key_exists($param, $post_data)) {
            $signatureString .= ':' . trim($post_data[$param]);
        } else {
            $signatureString .= ':';
        }
    }
    return sha1($signatureString);
}

// Build up the parameters needed by the gateway
$post_data = Array (
    'ivp_store'      => '[Your Store ID Goes Here]',
    'ivp_cart'       => 'Cart123',
    'ivp_amount'     => '299.00',
    'ivp_currency'   => 'AED',
    'ivp_test'       => '1',
    'ivp_timestamp'  => '0',
    'ivp_desc'       => 'Test Purchase',
    'ivp_extra'      => 'bill,return',
    'bill_title'     => 'Mr',
    'bill_fname'     => 'Test',
    'bill_sname'     => 'Customer',
    'bill_addr1'     => 'House name',
    'bill_addr2'     => 'Street name',
    'bill_addr3'     => 'Town',
    'bill_city'      => 'City',
    'bill_region'    => 'Region',
    'bill_zip'       => 'PostCode',
    'bill_country'   => 'AE',
    'bill_email'     => 'customer@email.com',
    'bill_phone1'    => '04 123 4567',
    'return_cb_auth' => '[Your Call-back URL goes here]',
    'return_cb_decl' => '[Your Call-back URL goes here]',
    'return_cb_can'  => '[Your Call-back URL goes here]',
    'return_auth'    => '[Your Return URL goes here]',
    'return_decl'    => '[Your Return URL goes here]',
    'return_can'     => '[Your Return URL goes here]',
);
$secret_key='[Your Secret Goes Here]'; // This must never be shown as part of the HTML

// First create the signature for the main purchase details, as this used both to authenticate
// the request and in creating the other signatures.
$post_data['ivp_signature']=SignData($post_data,$secret_key,
    'ivp_store,ivp_amount,ivp_currency,ivp_test,ivp_timestamp,ivp_cart,ivp_desc,ivp_extra');
// Now create the signature for the billing details (uses the ivp_signature created first)
$post_data['bill_signature']=SignData($post_data,$secret_key,
    'bill_title,bill_fname,bill_sname,bill_addr1,bill_addr2,bill_addr3,bill_city,bill_region, ' .
    'bill_country,bill_zip,ivp_signature');
// Now create the signature for the return/call-back URLs (also uses the ivp_signature)
$post_data['return_signature']=SignData($post_data,$secret_key,
    'return_cb_auth,return_cb_decl,return_cb_can, ' .
    'return_auth,return_decl,return_can,ivp_signature');

// Output the form fields. Ensuring that the form data is html safe (e.g. things like
// converting < to &lt; ) must be done after the signature values are calculated.
foreach ($post_data as $k => $v) {
    echo "<input type=\"hidden\" name=\"" . $k . "\" value=\"" . htmlspecialchars($v) . "\">";
}
?>
<input type="submit" value="Send Purchase Request"/>
</form></body></html>
```

The above example shows sending the basic purchase details along with the customer details (the customer may of already registered on your site, sending their details as part of the request removes the need for the customer to re-enter information they have already provided) and with the details of the URLs to be used for call-backs and the return addresses.

You must use the data your system receives within the call-back to update the order details, do not use the return URLs for this. Using the return URLs to update the order status opens up the possibility of the customer manually changing the URL in their browser location bar to change the status of an order within your system, and of order updates being missed should the customer not follow the return URL back to your site.

NOTE: The call-back system is a direct server to server connection, the customers' browser is not part of that request, and therefore any data such as cookies held by the browser will not be included. You should use information such as the cart ID to identify which order the call-back is for.

You can validate the call-back data using the same signature process (the SignData function shown above) and the same secret-key as was used when creating the transaction request, for example:

```
$secret_key='[Your Secret Goes Here]';

// Create a check value based on the secret key and the data received.
// To make the following more readable, the field list has been split over two lines
$hash_check=SignData($_POST,$secret_key,
    'auth_status,auth_code,auth_message,auth_tranref,auth_cvv,auth_avs,card_code,card_desc, '.
    'cart_id,card_desc,card_currency,card_amount,tran_currency,tran_amount,tran_cust_ip');

// Check that the signature in the message matches the expected value
if (strcasecmp($_POST['auth_hash'],$hash_check)!=0) {
    // Hash check does not match. Data may have been tampered with.
    die('Check mismatch');
}

// Hash check OK, use details supplied in POST data to determine what action to take
// $_POST['auth_status']
// A = Authorised, H = Authorised but on hold, any other character = not authorised
```

See the section on Transaction Results for more details on the fields that are provided as part of the call-back request.

If your systems do not receive any data as part of the call-back then please check the following:

- The URL must be internet accessible. Private URL/IP addresses cannot be used.
- The URL protocol must be either http or https.
- Only ports 80 or 443 can be used.

The process used to accept the call-back request must return with a status of '200 OK'. Other status codes will be treated as the call-back process not completing correctly. The process should handle the request as quickly as possible, as the customer will be waiting at the Transaction Processing page whilst the call-back is made.

Document history

Release	Changes
1.26	Added section on Alternate Payment Methods. Updated response codes.
1.25	Correction to the example code for checking call-back signature.
1.24	Added details on using alternate CVV values to simulate different transaction responses when in test mode.
1.23	Added example of checking the call-back signature using PHP. Updated response codes.
1.22	Added reference to the Payment Page Extensions guide, which contains details of the Repeat Billing options as well as the CardFilter and CardDiscount modules.
1.21	Card Filter options added
1.20	Added an example of generating a purchase request using PHP
1.19	Clarification on the use of mobile devices with the default purchase URL
1.18	Added flow charts showing the order that call-back and return URL's are used.
1.17	Added transparent mode as an additional method of processing transactions.
1.16	Updated response codes and supported currency codes.
1.15	Details of the options to set return and call-back URL's as part of the transaction request.
1.14	Test card details updated to show which cards will use the simulated 3D Secure authentication page.
1.13	Updated list of fields available as part of the call-back process.
1.12	Added details relating to the use of mobile devices.
1.11	Additional details relating to the use of the extra data fields (xtra_) that can be sent as part of the transaction request.
1.10	Additional information on the use of framed payment pages.
1.09	Added details relating to the use of framed payment pages.
1.08	Removed details relating to Solo cards – these cards are no longer in use.
1.07	Added examples of the currency selector and the 3D Secure authentication pages.
1.06	Added examples of the payment page layouts – single column and two column.
1.05	Added details on the use of the extra data fields (xtra_) as part of the transaction request.
1.04	Added details on sending delivery details (delv_) as part of the transaction request.
1.03	Added details of the test cards.
1.02	Formatting changes to section headers.
1.01	Added details on sending customer billing details (bill_) as part of the transaction request.
1.00	Initial release.