globalpayments

GLOBAL IRIS™

Powered by realex payments

Global Iris RealAuth – Hosted Payment Page

Developers Guide

October 2014

Version v1.1.1

Table of Contents

1 About This Guide

This section outlines the purpose and aim of the guide, target audience, any source materials or terminology used, and a general document description.

Please note that this document is regarded as confidential and is for customer use only. It has been supplied under the conditions of your payment processing contract.

1.1 Purpose

The purpose of this guide is to explain in detail what is involved in integrating with the Global Iris' Hosted Payment Page.

1.2 Audience

The target audience for this guide is software and web developers.

1.3 Prerequisites

In order to use this guide, you should have experience with and knowledge of HTML and at least one server side dynamic scripting language.

1.4 Related Documents

In addition to this guide, you can also refer to the following documents in the Global Iris documentation set for information about the RealAuth service:

- Sample Code: https://resourcentre.globaliris.com/downloads.html?id=117

1.5 Conventions

Global Iris documentation uses the following conventions:

Note: Tips or advice for the user.

Caution: Important note. Potential financial impact

Convention	Description	Example
Blue Italic or Plain Type	Hyperlinks and cross-references	https://hpp.globaliris.com/pay
Italics	Names of other guides	*RealAuth Developer's Guide*
Courier New	Program code, screen messages, directory files, and file names	<comments></comments>
Courier New	Placeholder for element names, field values, or user input	*card_holder_name*
BOLD CAPS	Error and warning messages	**101 / REFERRAL B**

2 Introduction

The Hosted Payment Page (HPP) is a simple and straightforward way of taking payments on your website. The HPP integration method is suitable for merchants that do not have their own secure server. Using this method, the customer will be redirected to Global Iris secure server to enter their details and complete the transaction. Because the customer is not entering any sensitive information on your own site, HPP meets your PCI obligations.

2.1 RealAuth Hosted Payment Page Features List

- The merchant does not need a secure server.
- The merchant's website can be hosted anywhere, and on any platform.
- The merchant does not collect their customer's payment details, and does not have access to them.
- The customer is redirected to the RealAuth application on a secure Global Iris server by a script on the merchant's website.
- Global Iris hosts a secure, merchant-branded web page. We collect the payment details and process the payment. The customer and the results of the transaction are sent back to the merchant via another script on the merchant's web site (Global Iris can provide sample scripts to get you started).

2.2 Prerequisites for Integration with HPP

In order to create a merchant account for the Hosted Payment Page, a merchant must provide:

- A Global Iris Merchant ID
- A sub-account name
- Referring and response URLs
- Bank merchant number (needed before your account can be set live)
- Shopping cart used on your website (if applicable).
- Details of any additional services required (RealMPI, DCC, RealVault)

2.3 PCI DSS Compliance (Card transactions only)

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard which dictates how sensitive details such as credit card numbers should be handled, stored and transmitted. The standard applies to all organisations that handle, store, process or exchange cardholder information from any card branded with the logo of one of the card brands (such as Visa and Mastercard). PCI DSS rules are administered by the card schemes and enforced by the acquiring banks who are members of said schemes.

Adherence to the PCI DSS is mandated by the merchant services agreement that you have signed with your acquiring bank, and is a condition of that agreement. Global Payments are a Level 1 PCI Compliant organisation, and submit to frequent audits of all of our systems and processes to ensure that this compliant status is upheld.

Global Payments’ compliant status extends to those merchants who use the Hosted Payment Page to take payments and do not handle, store or otherwise transmit card details in any other way. For more information on PCI DSS and your obligations as outlined under those rules, please refer to the PCI Council website - https://www.pcisecuritystandards.org/

3 HPP: Transaction Flow

Merchants who do not have their own secure server can use the RealAuth Hosted Payment Page. Rather than entering any sensitive information on a (non-secure) website, the customer is redirected to the Global Iris secure server. Here they are presented with a payment page that can be customised to maintain the appearance of your website. After entering their payment details and submitting the transaction, the Hosted Payment Page will send a response to your nominated response page. Your response page can then return a pre-defined message of your choice, depending on the outcome of the transaction. The customer will remain on the Global Iris server. The Hosted Payment Page can be customised using 'templates', which are described in Chapter 5.

There are two primary responsibilities of your response page during the transaction process (the response page is discussed in greater detail in Section 4.5):

1. To accept the response message received from Global Iris.

2. Output HTML to the screen. This is the message that is displayed to the customer depending on the success/failure of the transaction.

You may also wish to set up your response page to update your database, send emails, etc. upon receiving a successful transaction response.

Global Iris can supply working sample code in ASP, PHP, Java and Perl. Please note that this is sample code only and will need to be modified to suit your individual needs. The sample code will provide guidance on how to carry out the steps required for a Hosted Payment Page transaction to succeed.

The general flow of a Hosted Payment Page transaction is as follows:

1. A customer is shopping on your website. Once the customer has finished shopping and the full amount is known, the customer is presented with a “Proceed to Payment” page. This page is hosted on the merchant’s server.

2. If the customer confirms the transaction, a post request is sent to Global Iris, containing information about your merchant account and information about the transaction.

3. If the post is successful, the customer is redirected to the Hosted Payment Page on Global Iris’ secure server. The HPP is customisable to allow you to maintain the look-and-feel of your website. Here, the customer will be presented with the payment methods that your account is enabled for. If your account is only enabled for card payments, the customer will be immediately redirected to the card payment form.

4. After entering their details, the customer clicks Pay Now and the payment details are sent for processing. When the response from the bank is received, Global Iris sends a post response to a response script on your site (your response URL). The post response will include a result code and a message explaining whether the transaction was approved or declined. You can then choose to output HTML (which will be embedded in your template) depending on the result of the transaction. The customer is still on the Global Iris secure server at this time. The response page is displayed using the same template as the HPP.

Note: Customers must have Javascript enabled on their browser for HPP to function correctly.

Note: Requests should be sent to Global Iris only at the end of the shopping experience, once the total amount of the payment is known. No information about the contents of the order is required for Global Iris to process the transaction. However, you can send any information about the order to Global Iris – these will be ignored by the Global Iris system but will be sent back to your response script once the transaction has been processed.

It is worth noting that the Internet is not 100% reliable and communication errors may occur so it is possible that the information will not make it back to your response script. We recommend that an email with the order details and order ID be sent before the transaction is sent to the Global Iris application and another email with the result sent afterwards. In this way, details of an order that someone has actually been charged for should not be lost.

4 Integrating with HPP

4.1 HPP URLs

HPP has two separate URLs, one for live transactions, one for test transactions. When you first create an account with Global Iris, your account will be set to test mode. We recommend that you process several test transactions in test mode to confirm you are happy with how transactions are processing before setting your account live.
The URL for live transactions is: https://hpp.globaliris.com/pay
The URL for test transactions is: https://hpp.sandbox.globaliris.com/pay

4.2 Test Mode

HPP has a designated environment for testing purposes. The test environment is a replica of the live environment and offers all the functionality of the live environment without having to use actual live payment details (such as live card numbers). Global Iris highly recommend putting through several test transactions to ensure you are happy with all aspects of your integration with HPP. The crucial aspects of your integration to check before going live are:

- Your post to HPP is working correctly and you are being redirected to HPP upon submitting your transaction.
- Your template is rendering correctly on HPP for all payment methods.
- HPP is connecting correctly with your response page.
- Your response message is displaying correctly within your template.
- You can process both a successful and unsuccessful transaction from end to end.

Your Global Iris account manager can supply you with the correct test details to enable you to process transactions in the test environment. The test environment will be available for you to use even after your account has been switched to live mode.

Note: You can still process test transactions while in live mode. However, you cannot process live transactions while in test mode.

4.3 Post Request

To link your shopping cart to the Hosted Payment Page, you must insert hidden fields into a form that redirects to the Hosted Payment Page over a secure link. The page that contains the form that performs the post request is known as the “referring URL”. This URL needs to be emailed to globaliris@realexpayments.com to be added to the whitelist of permitted referring URLs for your account.
A typical implementation of the post request is shown below:

```
<form method="POST" action="https://hpp.globaliris.com/pay">
<input type="hidden" name="MERCHANT_ID" value="Global Iris
merchant-id">
<input type="hidden" name="ORDER_ID" value="unique order-id">
<input type="hidden" name="ACCOUNT" value="sub account name">
<input type="hidden" name="AMOUNT" value="amount">
<input type="hidden" name="CURRENCY" value="currency code">
<input type="hidden" name="TIMESTAMP" value="yyyymmddhhmmss">
<input type="hidden" name="SHA1HASH" value="40 character string">
<input type="hidden" name="AUTO_SETTLE_FLAG" value="1 or 0">
<input type="submit" value="Click here to Purchase">
</form>
```

Note: Test transactions are to be sent to: https://hpp.sandbox.globaliris.com/pay. Live transactions are to be sent to: https://hpp.globaliris.com/pay

Note: Some form of server side programming is required to create the SHA1HASH. All merchants will be required to perform some script configuration on their side. This is discussed further in Chapter 6.

4.4 HPP Request Field Definitions

The fields in the table below are accepted by Global Iris. Anything else will be returned back to your response script along with the Global Iris responses.

Field Title	Format	Length	M/O	Description
MERCHANT_ID	a-z A-Z 0-9 .	1-50	M	Supplied by Global Iris – **note this is not the merchant number supplied by your bank.**
ACCOUNT	a-z A-Z 0-9	0-30	O	The sub-account to use for this transaction. If not present, the default sub-account will be used.
ORDER_ID	a-z A-Z 0-9 _ -	1-40	M	A unique alphanumeric id that's used to identify the transaction. No spaces are allowed.
AMOUNT	0-9	1-11	M	Total amount to authorise in the lowest unit of the currency – i.e. 100 euro would be entered as 10000. If there is no decimal in the currency (e.g. JPY Yen) then contact Global Iris. No decimal points are allowed.
CURRENCY	a-z A-Z	3	M	A three-letter currency code (e.g. EUR, GBP). A list of currency codes can be provided by your account manager.
TIMESTAMP	0-9	14	M	Date and time of the transaction. Entered in the following format: YYYYMMDDHHMMSS. Must be within 24 hours of the current time.
SHA1HASH	a-f 0-9	40	M	A digital signature generated using the SHA-1 algorithm. See Chapter 6.
AUTO_SETTLE_FLAG	0 or 1	1	O	Used to signify whether or not you wish the transaction to be captured in the next batch. If set to "1" and assuming the transaction is authorised then it will automatically be settled in the next batch. If set to "0" then the merchant must use the RealControl application to manually settle the transaction. This option can be used if a merchant wishes to delay the payment until after the goods have been shipped.

				Transactions can be settled for up to 115% of the original amount and must be settled within a certain period of time agreed with your issuing bank. **Note: If you choose not to include the Autosettle field, the default behaviour will set the flag to “0”.**
COMMENT1	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | = ;	0-255	O	A freeform comment to describe the transaction.
COMMENT2	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | = ;	0-255	O	A freeform comment to describe the transaction.
RETURN_TSS	0 or 1	1	O	Used to signify whether or not you want a Transaction Suitability Score for this transaction. Can be “0” for no and “1” for yes. To maximise the usefulness of the RealScore you should also supply the next 7 fields.
SHIPPING_CODE	a-z A-Z 0-9 “” , . - / |	0-30	O	The postcode or ZIP of the shipping address.
SHIPPING_CO	a-z A-Z 0-9 “” , . -	0-50	O	The country of the shipping address.
BILLING_CODE	a-z A-Z 0-9 “” , . - / |	0-60	O	The postcode or ZIP of the billing address.
BILLING_CO	a-z A-Z 0-9 “” , . -	0-50	O	The country of the billing address.
CUST_NUM	a-z A-Z 0-9 – “” _ . , + @	0-50	O	The customer number of the customer. You can send in any additional information about the transaction in this field, which will be visible under the transaction in the RealControl application.
VAR_REF	a-z A-Z 0-9 – “” _ . , + @	0-50	O	A variable reference also associated with this customer. You can send in any additional information about the transaction in this field, which will be visible under the transaction in the RealControl application.
PROD_ID	a-z A-Z 0-9 – “” _ . , + @	0-50	O	A product id associated with this product. You can send in any additional information about the transaction in this field, which will be

				visible under the transaction in the RealControl application.
HPP_LANG	ISO 639-1	2	O	Used to set what language HPP is displayed in. Currently HPP is available in English, Spanish and German, with other languages to follow. If the field is not sent in, the default language is the language that is set in your account configuration. This can be set by your account manager.
MERCHANT_RESPONSE_URL	a-z A-Z 0-9 ' , + . _ - & \ / ? % : $ & # =	0-255	O	Used to set which URL that Global Iris will send the transaction response to. When you are creating your account with Global Iris , you will be asked to provide a response URL for your account. If this field is sent in the post request, it takes precedence over the response URL set on your Global Iris account. If Global Iris cannot connect to this URL, the response URL set on your account will be attempted.
CARD_PAYMENT_BUTTON	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	0-25	O	Used to set what text is displayed on the payment button for card transactions. If this field is not sent in, “Pay Now” is displayed on the button by default.
ANYTHING ELSE	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	0-255	O	Anything else you send to Global Iris will be returned in the response (whatever other information you collected from the customer such as product or address/telephone numbers etc….)**.**

The following indicators are used to show whether or not an element is required or optional.

M	Required for this request type
O	Optional
C	Required depending on another optional field

4.5 HPP Response Field Definitions

Response data is sent back to your response script for each transaction. After the customer has completed their transaction on the Hosted Payment Page, our application calls your response script with the response details. You can use this response to display HTML on your response page, update your own database and send emails to your customers based on the result of the transaction.

In order to receive this data you must provide Global Iris with the URL of your response script. The response URL is to be emailed to globaliris@realexpayments.com. This script must only return text as output – if image tags are included there will be a popup warning about mixed secure/insecure content on the page. The template that was used for the HPP transaction will be used again for this page. You should include a link that continues the customers shopping experience. Again, we can provide working sample code that will make this process easier.

Successful transactions on HPP will receive a “00” result code. In this case, your response page should output some HTML informing the customer that their transaction has been successful. Unsuccessful transactions that have a result code beginning with 1 (e.g. 101) will also be returned to your response script. Your response script should be robust enough to deal with unsuccessful transaction result codes and react accordingly. For example, you could prompt the customer to try another card and provide a link to return them to HPP.

For transactions that receive a result code of 200 and above, HPP does not post back to your response script. Instead, an error code and respective message will be displayed on screen to the customer.

Note: If you do choose to return the customer to HPP after an unsuccessful transaction, you must ensure that a unique Order ID is used. Any Order ID that has been processed previously will receive a duplicate Order ID error.

Here is an example of a response for a successful card transaction:

```
MERCHANT_ID=thestore
ACCOUNT=internet
ORDER_ID=ORD453-11
TIMESTAMP=20130814122239
AMOUNT=5000
COMMENT1=WQYRhW4Kydrb7mBzCeXvh7AePE
COMMENT2=NtrNfwhCZc397t73ZPNzXJb75h
SHA1HASH=d0040af429b6be5b315fb660c585727d3abe7e5a
RESULT=00
AUTHCODE=123420
MESSAGE=AUTH CODE: 123420
PASREF=13649024563820
AVSPOSTCODERESULT=U
AVSADDRESSRESULT=U
CVNRESULT=M
BATCHID=870
```

The response fields are as follows:

Field Title	Description
MERCHANT_ID	This is the merchant id that Global Iris assigns to you.
ACCOUNT	The sub-account used in the transaction.
ORDER_ID	The unique order id that you sent to us.
TIMESTAMP	The date and time of the transaction.

Field Title	Description
AMOUNT	The amount that was authorised. Returned in the lowest unit of the currency.
AUTHCODE	Will contain a valid authcode if the transaction was successful. Will be empty otherwise.
RESULT	The outcome of the transaction. Will contain “00” if the transaction was a success or another value (depending on the error) if not.
MESSAGE	Will contain a text message that describes the result code above.
CVNRESULT	The result of the Card Verification check (if enabled): M: CVV Matched. N: CVV Not Matched. I: CVV Not checked due to circumstances. U: CVV Not checked – issuer not certified. P: CVV Not Processed.
PASREF	A unique reference that Global Iris assign to your transaction.
BATCHID	This is the Global Iris batch that this transaction will be in. (This is equal to “**-1**” if the transaction was sent in with the autosettle flag off. After you settle it (either manually or programmatically) the response to *that* transaction will contain the batch id.)
ECI	This is the ecommerce indicator (this will only be returned for 3DSecure transactions).
CAVV	Cardholder Authentication Verification Value (this will only be returned for 3DSecure transactions).
XID	Exchange Identifier (this will only be returned for 3DSecure transactions).
SHA1HASH	A SHA-1 digital signature created using the above fields and your shared secret. Needs to be sent in lowercase.
COMMENT1	Whatever data you have sent in the request will be returned to you.
COMMENT2	Whatever data you have sent in the request will be returned to you.
TSS	The Transaction Suitability Score for the transaction.
TSS_*idnum*	The Real**Score** is comprised of various distinct tests. Using the Real**Control** application you can request that Global Iris return certain individual scores to you. These are identified by numbers - thus **TSS_1032** would be the result of the check with id 1032. You can then use these specific checks in conjunction with Real**Score** score to ascertain whether or not you wish to continue with the settlement.
ANYTHING ELSE	Anything else you sent to us in the request will be returned to you.

Note: Additional fields may be returned to your response page by HPP as new functionality is added. Your response script should be designed in such a way to allow for these additional fields.

4.6 Displaying Custom Text on HPP

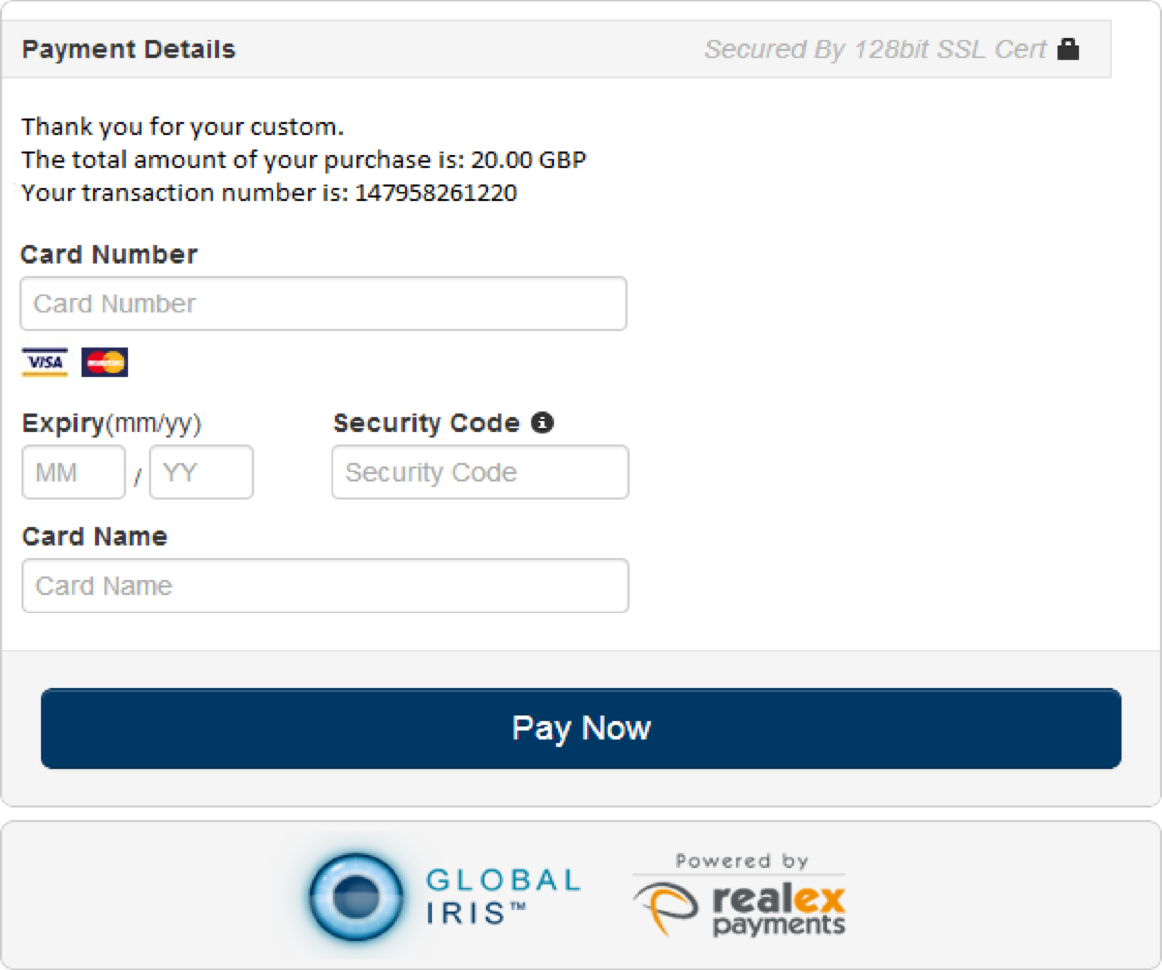
4.6.1 Information Text

HPP allows you to add your own customisable text to the payment page using simple HTML via the Global Iris reconciliation tool, RealControl. With HPP, you can dynamically display information such as the Order ID and the total amount and currency of the transaction to your customers while they are on the payment page. You can use the RealControl information text to display however you wish, a simple example is displayed below.

Instructions on how to display this text using RealControl is included in the *Global Iris RealControl User Guide*.

The following tags can be used to dynamically display information sent in the post request on HPP:

- **<#ORDER_ID#>:** Displays the information sent in the ORDER_ID post field.
- **<#TOTAL#>:** Displays the value sent in the AMOUNT field in the post request. This will also display the currency that the transaction was processed for.
- **<#COMMENT_1#>:** Displays the information sent in the COMMENT1 post field.
- **<#COMMENT_2#>:** Displays the information sent in the COMMENT2 post field.



Thank you for your custom.
The total amount of your purchase is: 20.00 GBP
Your transaction number is: 147958261220

4.6.2 Success and Failure Text

For every transaction that you process on HPP, Global Iris will send a post response to your response script. In the event that Global Iris cannot connect to your response script, you can set the text to be displayed to your customers for both successful and failed transactions via RealControl. These messages will be displayed within the template that you have provided to your Account Manager. See Chapter 5 for more information on templates.

Instructions on how to display this text using RealControl is included in the *Global Iris RealControl User Guide*.

5 Templates

To allow the Hosted Payment Page to maintain the look-and-feel of your website, you will need to have a template page, optionally with images/style sheets uploaded to the Global Iris servers. All templates should be sent to Global Iris support via e-mail (globaliris@realexpayments.com).

The Hosted Payment Page allows you to upload two templates for each sub-account you have created; a standard template for rendering on all desktop/laptop devices, and a mobile-aware template for rendering on mobile devices. The Hosted Payment Page will automatically render the correct template depending on what device your customer is using. Templates can also be uploaded to your account at merchant level, so if you have multiple sub-accounts, the same template will be rendered on all of these accounts. The templates sent to Global Iris should match the criteria listed in the following sections. If you do not provide Global Iris with a template, a basic template will be provided for you for both mobile and non-mobile devices.

5.1 Desktop and Tablet Templates

The basic structure of a template is shown below. Note the HTML tag **<hpp:body />** that indicates where the payment form should be placed; this tag **must** be present in your template page.
The template should resemble the rest of the shopping experience of your website so that the customer does not immediately realise that they have been redirected away from your site, but, as a secure encrypted connection will be used, there should be as few images as possible. A typical template may consist of: a 'header' image, a plaintext message for the customer and the required **"<hpp:body />"** tag. Simply using the general colour scheme of the other pages in your shopping cart is quite effective.

Below is an example of a simple template that could be applied to your account:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Your title</title>
<link rel="stylesheet" type="text/css" href="style.css">
</head>
<body>
<div id="wrapper">
<div id="banner">
<img src="logo.jpg" width="750" height="201" alt="My Logo" hspace="0" vspace="0" border="0"
align="top">
</div>
<div id="infoBar">Secure Payment</div>
<div><br>
<hpp:body />
</div>
</div>
</body>
</html>
```

Below are the full requirements for the template page:

1. The template **must** be written in valid, semantic HTML. You can validate your HTML at the following URL: http://validator.w3.org/

   Note: You should validate your HTML before inserting the **<hpp:body />** into your form as this tag will cause the HTML to fail validation.

2. Template pages must contain the payment form tag **<hpp:body />**
3. All images or CSS used in the template must be referred locally on our server. There should be no absolute URLs to external images or CSS. This means that you will need to send the image files to us along with the template page.
4. All resources used by the desktop template (CSS, images) should be placed in a folder called "desktopresources". The folder structure within this folder can be however you wish.
5. There can be no scripting of any kind in the template for security reasons. It should contain only basic HTML.
6. The name of the file **must** be: "desktop.html".
7. Only HTML, CSS, JPG, PNG, GIF, ICO and CSS font files are permitted.
8. The maximum size of an individual file is 262KB.

5.2 Mobile Templates

If a customer is redirected to the HPP from your website while using a mobile device, HPP can detect this and render a mobile-aware template for such devices. If you do not have a mobile aware template uploaded for this account Global Iris will provide a basic mobile-aware template displaying the card payment form.

The same rules apply for mobile-aware templates as non-mobile templates. You are permitted to display multiple images and CSS on screen. However, when dealing with mobile devices, due to the small nature of them, and the limited screen real estate available, it is strongly recommended to use a basic mobile template to ensure the payment form is the most prominent part of the page. Your company logo displayed at the top of the payment form should suffice as your mobile template.

There is an additional tag to be placed in the <head> of your HTML page for mobile-aware templates to ensure the payment form renders correctly. The additional tag is:

<meta name="viewport" content="width=device-width, initial-scale=1">

This tag will ensure that the payment form will display to the correct scale of the device that your customer is using.

The requirements for mobile aware templates are as follows:

1. Mobile aware templates should include the new tag: **<meta name="viewport" content="width=device-width, initial-scale=1">** within the <head> of the template.
2. The template **must** be written in valid, semantic HTML. You can validate your HTML at the following URL: http://validator.w3.org/

   Note: You should validate your HTML before inserting the **<hpp:body />** into your form as the this tag will cause the HTML to fail validation.

3. Template pages must contain the payment form tag **<hpp:body />**
4. All images or CSS used in the template must be referred locally on our server. There should be no absolute URLs to external images or CSS. This means that you will need to send the image files to us along with the template page.
5. There can be no scripting of any kind in the template for security reasons. It should contain only basic HTML.
6. The name of the file **must** be: "mobile.html".

7. Only HTML, CSS, JPG, PNG, GIF, ICO and CSS font files are permitted.
8. The maximum size of an individual file is 262KB.

Here is an example of an acceptable HPP template for mobile devices:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1">
<title>Your title</title>

</head>

<body>

<div id="banner">

<img src="logo.jpg" align="top">

</div>

<div><br>

<hpp:body />

</div>

</body>

</html>
```

6 Security

6.1 Referring URLs

In order to integrate with the HPP live environment, it is necessary to provide Global Iris with a list of your referring URLs.

Your referring URL is the page that posts the transaction data to Global Iris. Multiple referring URLs can be assigned to your account. Global Iris maintains a white-list of Referring URLs that transactions can be processed against your account from. Any request coming from a URL not on this white-list will result in an error message and the transaction will not continue. Your referring URL(s) can be sent to: globaliris@realexpayments.com. Referring URLs are not checked when your account is in test mode.

6.2 Request Hash

To ensure that the post request Global Iris receives comes from you we require that you send us a hash of certain elements (specifically the TIMESTAMP, MERCHANT_ID, ORDER_ID, AMOUNT, and CURRENCY) which are in turn hashed with a piece of information called a shared secret. The hashing algorithm used by HPP is SHA-1.

The SHA-1 algorithm is a secure hash function. It takes a string as input, and produces a fixed size number - 160 bits. This number is a hash of the input, and a small change in the input results in a substantial change in the output. The function is thought to be secure in the sense that it requires an enormous amount of computing power and time to find a string that hashes to the same value. In others words, there's no way to decrypt a secure hash.

Here is a sample request:

```
<input type="hidden" name="MERCHANT_ID" value="thestore">
<input type="hidden" name="ACCOUNT" value="internet">
<input type="hidden" name="ORDER_ID" value="ORD453-11">
<input type="hidden" name="AMOUNT" value="29900">
<input type="hidden" name="CURRENCY" value="EUR">
<input type="hidden" name="TIMESTAMP" value="20130814122239">
<input type="hidden" name="AUTO_SETTLE_FLAG" value="1">
```

To construct the hash follow this procedure:

Form a string by concatenating the above fields with a period (“.”) in the following order (**TIMESTAMP.MERCHANT_ID.ORDER_ID.AMOUNT.CURRENCY**)

Like so:

(20130814122239**.thestore.ORD453-11.29900.EUR**)

Get the hash of this string (SHA-1 shown below).

(**ed89cdf884e2fa9abf4ab1bb621ac1f1b19b988c**)

It is important that you convert this to lowercase letters. The output from the SHA1 function will give different answers in the next step if you use uppercase letters.

Create a new string by concatenating this string and your shared secret using a period. You will be assigned a shared secret when you have set up an account with Global Iris.

(**ed89cdf884e2fa9abf4ab1bb621ac1f1b19b988c.mysecret**)

Get the hash of this value. This is the value that you send to Global Iris.
(**cc72c08e529b3bc153481eda9533b815cef29de3**)

```
<input type="hidden" name="SHA1HASH" value="cc72c08e529b3bc153481eda9533b815cef29de3">
```

When Global Iris receives the request, we perform the same procedure on the five pieces of information and your shared secret (which we have stored in our database). If the resulting hash is the same as the one that you sent us then the data could only have been sent by someone that had your shared secret.

Thus it is very important to keep this shared secret protected. Shared secrets should never be sent via email or text.

6.3 Response Hash

When Global Iris is responding, we will send you a hash of the response elements in the same way so that you can confirm that the response came from Global Iris. (This will be a hash of the TIMESTAMP, MERCHANT_ID, ORDER_ID, RESULT, MESSAGE, PASREF and AUTHCODE with your secret key).

The response hash is constructed as follows:

Form a string by concatenating the above fields with a period (“.”)
(20130814122239**.thestore.ORD453-11.00.Successful.3737468273643.79347**)

Get the hash of this string (SHA-1 shown below).
(**e7aacea30a56a7d0dac4eb6f956ab6337f507c90**)

Create a new string by concatenating this string and your shared secret using a period.
(**e7aacea30a56a7d0dac4eb6f956ab6337f507c90.mysecret**)

Get the hash of this value. This should be the same as the value you receive from Global Iris.
(**f093a0b233daa15f2bf44888f4fe75cb652e7bf0**).

7 Card Transactions

The Hosted Payment Page can accept transactions from all major card types, depending on your Merchant Services Agreement with your Acquiring Bank.

7.1 The Card Payment Form

The card payment form is where the customer enters their card details in order to process a card payment. There are four fields to be filled in, if any of them are missing or invalid, the transaction cannot process. The fields are:

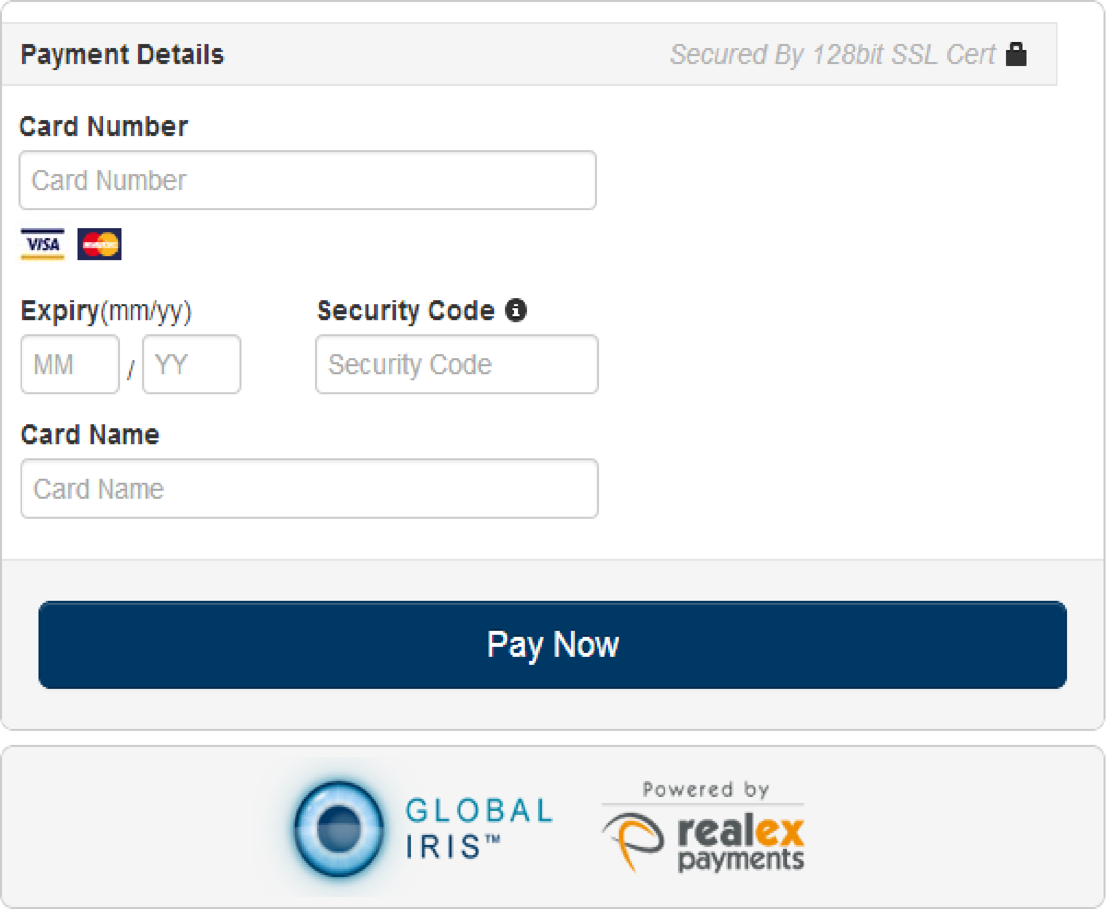
- Card Number
- Expiry Date
- Security Code
- Card Name

Card Number: The customer enters in their card number in this field. The field will only accept numeric values, any non-numeric characters will not be allowed. Card numbers must be between 12 and 19 digits in length, otherwise an error message will be displayed. The HPP will display the logos of all card types your account is enabled to take transactions for as per your Merchant Services Agreement. HPP will detect the type of card from the card's BIN, after which the logo of that card type will remain highlighted and all other card types will be greyed out. A Luhn check (an algorithm used to identify valid card numbers) is also performed on any card number entered. If a card number fails this check, an error message will be displayed to the customer and the transaction will not be allowed to continue.

Expiry Date: The expiry date is another required field, located on the front of a customer's card. The Expiry Date field again will only accept numeric characters, non-numeric characters will not display. The expiry date must contain two digits to represent the month and two digits to represent the year. It cannot be in the past or an error message will be displayed to the customer.

Security Code: The security code (CVN), is an additional 3 digit code (4 digits for American Express) on the front of a customer's card. Again, the form accepts numeric characters only, either 3 or 4 digits in length; otherwise an error is displayed to the cardholder.

Card Name: A text field that will accept both alphabetic and numeric characters, up to 100 characters in length. The card name field cannot be empty; otherwise the transaction will not be allowed to continue.



Payment Details

Secured By 128bit SSL Cert

Card Number

Card Number

Expiry(mm/yy)

MM / YY

Security Code

Security Code

Card Name

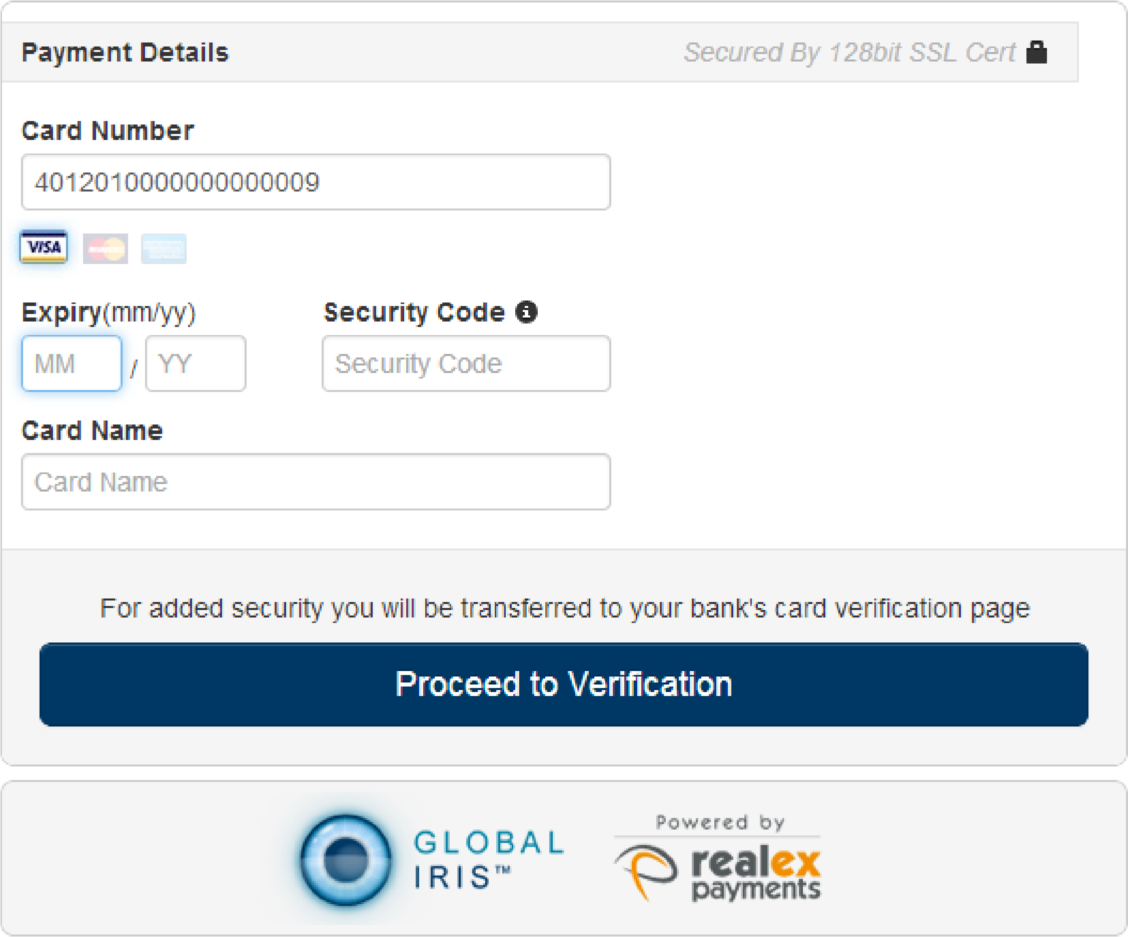
Card Name

7.2 3D Secure

3D Secure is the generic name given to the cardholder authentication scheme developed by the card schemes. Visa branded their implementation "Verified by Visa" (or VbyV), MasterCard branded theirs "SecureCode" and American Express' implementation is called "Amex SafeKey". The process involved is identical for Visa and MasterCard. Amex SafeKey do not accept liability shift for the first scenario, outlined below. 3D Secure was introduced as a means to reduce the risk of chargebacks for merchants by shifting the liability of the transaction on to the cardholder. RealMPI is the service used by Global Iris to implement the 3D Secure process.

3D Secure involves the cardholder authenticating themselves by entering their correct 3D Secure passphrase that they have set up with their issuing bank. When the cardholder enters in their passphrase correctly, they can no longer claim that the transaction wasn't processed by them as only they are supposed to know their own passphrase. Further information on 3D Secure is available in our *Global Iris RealMPI Overview Guide*.

HPP enables you to use the 3D Secure service without any additional set up on your side. If your account has been enabled for 3D Secure, when the cardholder enters their card number, upon exiting the field, HPP will make a request to check to see if their card is enrolled for 3D Secure or not. If the cardholder has enrolled their card for 3D Secure, the "Pay Now" button will appear as "Proceed to Verification" and the cardholder will be informed that they will be transferred to their Issuing Bank's site to confirm their passphrase.



Payment Details

Secured By 128bit SSL Cert

Card Number

4012010000000000009

Expiry(mm/yy)

MM / YY

Security Code

Security Code

Card Name

Card Name

For added security you will be transferred to your bank's card verification page

Upon clicking the "Proceed to Verification" button, HPP will automatically redirect the cardholder to their bank to enter their passphrase. If they enter their correct password, and the transaction is approved, the cardholder will be redirected back to your response page. A post response will be sent to your response script, with additional 3D Secure values: ECI, XID and CAVV (see Section 4.5 HPP Response Field Definitions).

There are 10 scenarios that can occur during the 3D Secure process. Three of these scenarios allow you to avail of a shift in liability in the event of a chargeback occurring from a fraudulent transaction. It is up to you which scenarios you wish to accept transactions for, however Global Iris strongly recommend that you only proceed with transactions where the full shift in liability is afforded to you. In scenarios 1 and 6, the issuing bank is liable for the chargeback. In scenario 5, the customer is liable. Please contact Global Iris to discuss the 3D Secure configuration options.

Below is a table of the possible scenarios, showing which scenarios are the ones where you can avail of the shift in liability in the event of a chargeback from a fraudulent transaction.

Scenario	Title	Description	Action
1	Cardholder Not Enrolled	The card holder is not enrolled in the 3dsecure service.	Shift in liability **Note:** Amex does not offer Shift in liability.

Scenario	Title	Description	Action
2	Unable To Verify Enrolment	The bank's enrolment server is temporarily down, so Global Iris cannot check if the cardholder is enrolled.	No Shift in liability
3	Invalid Response From Enrolment Server	The bank's enrolment server has sent back an invalid response Global Iris. Global Iris cannot check if the card holder is enrolled.	No Shift in liability
4	Enrolled, But Invalid Response From ACS (Access Control Server)	The card holder is enrolled but the response from the banks website has been tampered with. This should be treated as a fraudulent transaction.	No Shift in liability
5	Successful Authentication	The card holder is enrolled and has entered their passphrase correctly.	Shift in liability
6	Authentication Attempt Acknowledged	The card holder is enrolled but the bank doesn't have the facility to check the passphrase and so acknowledge the authentication attempt.	Shift in liability
7	Incorrect Password Entered	The card holder is enrolled but has entered the incorrect password. The card holder has not been authenticated.	No shift in liability
8	Authentication Unavailable	The card holder is enrolled but the bank’s website is temporarily unavailable. Cannot continue with the authentication.	No shift in liability
9	Invalid Response From ACS	The card holder is enrolled, but the banks website has sent back an invalid response to Global Iris. Cannot continue with the authentication	No shift in liability
10	RealMPI Fatal Error	The RealMPI service is temporarily down.	No shift in liability

Note: If a transaction is processed through your account that triggers one of the scenarios that you have set up to reject, HPP will send a post back to your response script with a Result Code of 110 and a relevant error message. The transaction will not be processed.

8 Card Storage

8.1 Overview

RealVault is Global Iris' card storage solution. Using RealVault enables you to enhance your customer's shopping experience by saving their card details for future purchases, while also alleviating any PCI compliance related issues associated with card storage. By using Global Iris to store your card details, you can save on both time and cost.

When using RealVault, each customer is assigned a unique token reference (a “Payer Reference”). A payer can then have multiple payment methods (for example, if they have both a Visa and Mastercard). Payment Methods are identified by a “Payment Reference”, which must be unique to that Payer Reference. The card details are stored on Global Iris‘servers, removing any PCI compliance issues on your side.

Any future transactions you wish to process against a customer can then be referenced by the Payer Reference and Payment Reference, rather than the card details themselves. HPP enables you to save your customer's card details when they enter them on the payment form, but all future transactions against that customer must be processed via RealVault XML API.

Note: RealVault is a chargeable service, please consult your Global Iris account manager if you wish to avail of this service.

8.2 Post Request

To begin saving your customer's card details with HPP, some additional fields must be sent in your post request to Global Iris. These are:

```
<input type="hidden" name="OFFER_SAVE_CARD" value="1">
<input type="hidden" name="PAYER_REF" value="myshop">
<input type="hidden" name="PMT_REF" value="mycard1">
<input type="hidden" name="PAYER_EXIST" value="0">
<input type="hidden" name="CARD_STORAGE_ENABLE" value="1">
```

8.3 Card Storage Request Field Definitions

Field Title	M/O	Format	Length	Description
CARD_STORAGE_ENABLE	*M*	0 or 1	1	This field determines whether RealVault is activated or not. If it is set to “1” then card storage is enabled, if set to “0” then it is not.
OFFER_SAVE_CARD	*M*	0-9	1	This hidden field determines whether or not to show the “Save Card Details” tick box to the customer. If this field is set to “1” then the tick box is shown, if set to “0” then it is not.
PAYER_REF	*O*	a-z A-Z\ 0-9 _	1-50	This field contains the payer reference used for this cardholder. If this field is empty or missing and PAYER_EXIST = 0, then a

Field Title	M/O	Format	Length	Description
				PAYER_REF will be automatically generated. To add another card to an existing payer the PAYER_REF field should be set to their existing payer reference. This field is mandatory if the CARD_STORAGE_ENABLE is set to 1 and the PAYER_EXIST flag is set to 1. If PAYER_EXIST = 1 and CARD_STORAGE_ENABLE = 1, a 5xx error will be returned if the field is empty or missing: 5xx “Mandatory field missing. PAYER_REF not present in request”. **Global Iris suggests that the merchant supplies the payer reference as it will be easier for the merchant to manage their payers.**
PMT_REF	*O*	a-z A-Z 0-9	1-30	The reference to use for the payment method saved. If this field is not present an alphanumeric reference will be automatically generated. **Global Iris suggests that the merchant supplies the payment reference as it will be easier for the merchant to manage their payers.**
PAYER_EXIST	*M*	0-9	1	If you wish to **add** a new card to an existing payer, this field should be set to “1”. Otherwise this should be set to “0”, i.e. if it is a new payer. If the payer exists and the value is set to “1”, Global Iris will not create a new payer, but will add the new card used to the payer specified in the PAYER_REF field.
RECURRING_TYPE	*C*	a-z A-Z	See Description	If you are saving the card information for use in a recurring payments / continuous authority manner, then you must set the RECURRING_TYPE and RECURRING_SEQUENCE fields. RECURRING_TYPE is either

Field Title	M/O	Format	Length	Description
				fixed or **variable** depending on whether the amount will change for each transaction. Please speak to your Integration and Support analyst about these fields, as in most cases these will not need to be included.
RECURRING_SEQUENCE	*C*	a-z A-Z	See Description	This must be set to **first**. Please speak to your account manager about these fields, as in most cases these will not need to be included.

The following indicators are used to show whether or not an element is required or optional.

M	Required for this request type
O	Optional
C	Required depending on another optional field

8.4 Card Storage Response Field Definitions

When using RealVault with HPP, you will receive extra fields in the response post that is sent to your response script after each transaction. These extra fields are described below.

Field Title	Description
REALWALLET_CHOSEN	This field indicates to the merchant if the cardholder has chosen to have their card details saved. If the field is set to 1 then the cardholder asked to have the card details stored, if not chosen the field is set to 0. This way the merchant knows what option the cardholder took. This field is always returned if the merchant submits the request field **OFFER_SAVE_CARD = 1**
PAYER_SETUP	Whether or not the cardholder was set up on the Global Iris System as a payer. A value of “00” implies a successful setup and any other value indicates an error – usually a 508. **The field is only returned if a payer set up was attempted i.e. this field is not returned if the request involves setting up an existing payer with a new payment method.**
PAYER_SETUP_MSG	This field indicates the message text returned by Global Iris as a result of the cardholder being set up as a payer. **The field is only returned if a payer set up was attempted i.e. this field is not returned if the request involves setting up an existing payer with a new payment method.**
PMT_SETUP	Whether or not the cardholder’s card details were set up. A value of “00” implies a successful setup and any other value indicates an error. **The field is only returned if a card payment method was attempted.**
PMT_SETUP_MSG	This field indicates the message text returned by Global Iris as a result of the card payment details being set up on the Global Iris system.

Field Title	Description
	The field is only returned if the card payment method set up was attempted.
SAVED_PAYER_REF	The payer reference given to this cardholder. If the PAYER_REF field was present in the incoming hidden fields then this field will be equal to that. Otherwise this field will be an automatically generated alphanumeric value. **This field will only be returned if the payer and payment references were successfully set up.**
SAVED_PMT_REF	The card payment reference for this payment method. This is an alphanumeric reference. If the PMT_REF field was specified in the incoming hidden fields, then this field will be equal to that. Otherwise this field will contain an automatically generated alphanumeric value. **This field will only be returned if the payer and payment references were successfully set up.**
SAVED_PMT_TYPE	The card type of payment saved. This is the card type of the card payment method stored. **This field will only be returned if the payer and payment references were successfully set up.**
SAVED_PMT_DIGITS	This field will contain some masked digits from the card payment method card number for display purposes, e.g. 664422xxxx7820. **This field will only be returned if the payer and payment references were successfully set up.**
SAVED_PMT_EXPDATE	This will contain the expiry date of the card payment method for display purposes. This can also be used to alert cardholders to the impending expiration of their saved card details. It will be in the format MMYY, e.g. 1108. **This field will only be returned if the payer and payment references were successfully set up.**
SAVED_PMT_NAME	The name of the person associated with the payment method – i.e. the card holder name. This is for display purposes. **This field will only be returned if the payer and payment references were successfully set up.**

8.5 Using RealVault on HPP

When using RealVault on HPP, there are three scenarios that you can offer your customers when they reach the card payment form. These are:

1. Offer your customer the choice to save their card details.
2. Automatically save the customer’s card details without offering them the choice.
3. Don’t save the customer’s card details.

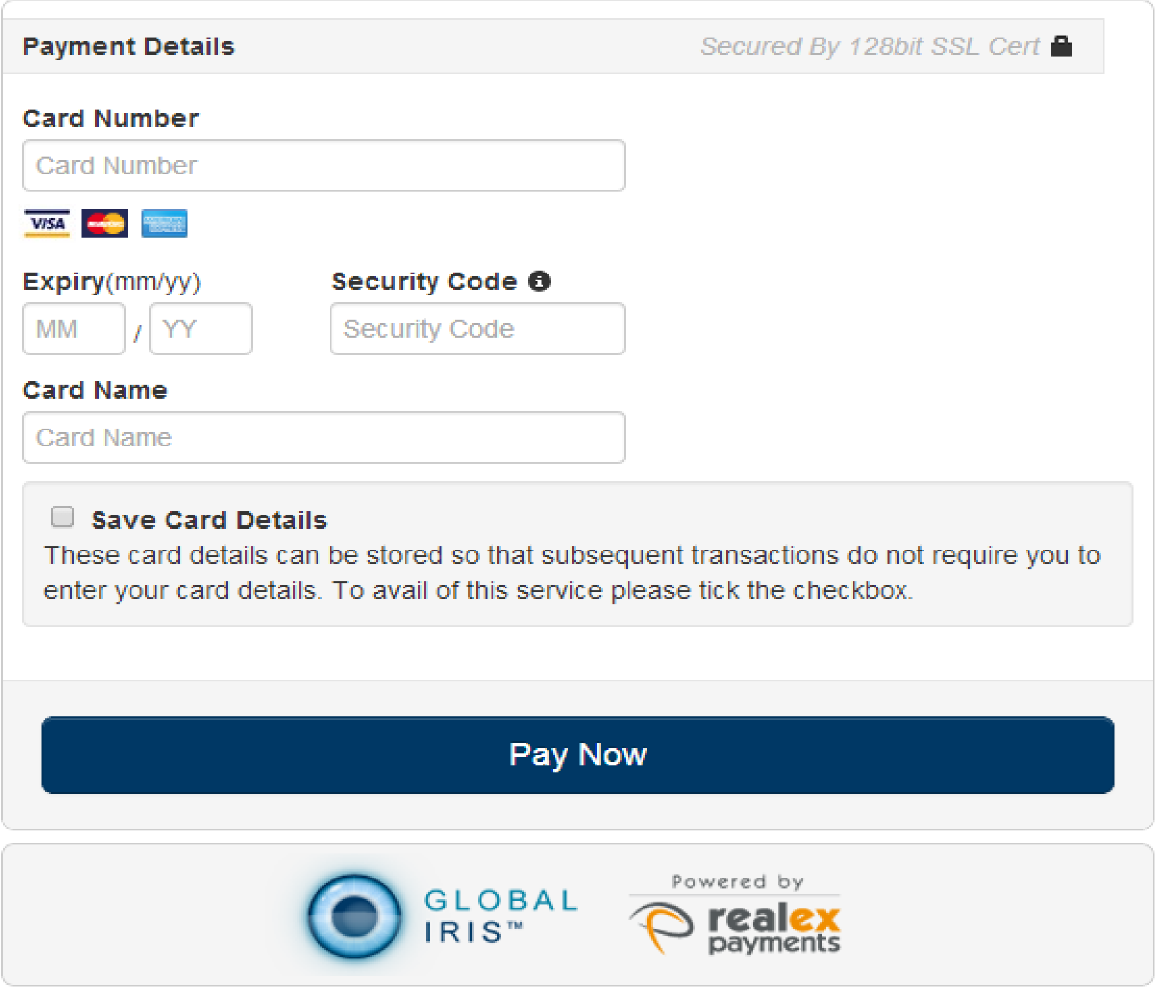
Note: Card details will only be stored if the initial authorisation is successful.
These three scenarios are controlled using the two field inputs, CARD_STORAGE_ENABLE and OFFER_SAVE_CARD. They are implemented as follows:

CARD_STORAGE_ENABLE	OFFER_SAVE_CARD	Description
1	1	Card storage enabled. Checkbox displayed to the customer. Card details will be stored

CARD_STORAGE_ENABLE	OFFER_SAVE_CARD	Description
		if customer selects the checkbox. If not, card details will not be saved. (Scenario 1)
1	0	Card storage enabled. Checkbox not displayed to the customer. Card details will be stored automatically. (Scenario 2)
0	0	Card Storage disabled. Checkbox not presented to customer. (Scenario 3)
0	1	Error thrown.

8.5.1 Offering Customers the Option to Save Card Details

As detailed above, if you wish to offer your customer the choice to save their card details, you must set both CARD_STORAGE_ENABLE and OFFER_SAVE_CARD to 1. When the customer reaches the card payment screen, they will be presented with the following screen:



These card details can be stored so that subsequent transactions do not require you to enter your card details. To avail of this service please tick the checkbox.

If the customer chooses to select the checkbox, their card details will be saved. If they do not select the checkbox, their card details will not be stored.

8.5.2 Automatically Saving Card Details

If you wish to automatically save your customer's card details, you must set CARD_STORAGE_ENABLE = 1 and OFFER_SAVE_CARD = 0. In this scenario, no checkbox will be displayed to the customer.
Note: As the merchant, you are obliged to inform your customers that their card details are being stored.

8.5.3 Not Saving Card Details

By setting CARD_STORAGE_ENABLE AND OFFER_SAVE_CARD to 0, no checkbox will be displayed to your customers and their card details will not be stored.

8.6 HPP RealVault Response Scenarios

There are three scenarios that can happen when a customer attempts to store their card details. These are:

1. The transaction was successful and card details were successfully stored.
2. The transaction was successful but there was an error storing the card details.
3. The transaction was not successful.

For each of these scenarios, the customer must be notified whether or not the transaction was successful and whether or not their card details were stored by displaying the appropriate text using your response script. You can determine the success or failure of the transaction and payer or payment method setup by examining the transaction response.

8.6.1 Transaction Successful, Card Details Stored Successfully

RESULT=00	The result of the authorisation request
PAYER_SETUP=00	The result of the payer new XML generated by the redirect service following the successful authorisation of the card.
PAYER_SETUP_MSG	Successful
PMT_SETUP=00	The result of the card new XML generated by the redirect service following the successful set up of the payer.
PMT_SETUP_MSG	Successful

In this instance, the merchant should expect to see the following elements returned in the response:

```
REALWALLET_CHOSEN=1
PAYER_SETUP=00
PAYER_SETUP_MSG=Successful
SAVED_PAYER_REF=pgtestpayer4
PMT_SETUP=00
PMT_SETUP_MSG=Successful
SAVED_PMT_TYPE=VISA
SAVED_PMT_REF=123
SAVED_PMT_DIGITS=664422xxxx1307
SAVED_PMT_EXPDATE=0212
SAVED_PMT_NAME=Joe Bloggs
RESULT=00
```

8.6.2 Transaction Successful, Error Storing Card Details

8.6.2.1 Payer Setup Fail: Payer Already Exists

RESULT=00	The result of the authorisation request
PAYER_SETUP=508	The result of the payer new XML generated by the redirect service following the successful authorisation of the card.
PAYER_SETUP_MSG	That payer reference already exists
PMT_SETUP=508	The result of the card new XML generated by the redirect service following the successful set up of the payer.
PMT_SETUP_MSG	Error creating payer - payment method aborted

In this instance, the merchant should expect to see the following elements returned in the response:

```
REALWALLET_CHOSEN=1
PAYER_SETUP=508
PAYER_SETUP_MSG=That payer reference already exists
PMT_SETUP=508
PMT_SETUP_MSG=Error creating payer - payment method aborted
RESULT=00
```

8.6.2.2 Payment Setup Fail: Payment Reference Already Exists

RESULT=00	The result of the authorisation request
PAYER_SETUP=00	The result of the payer new XML generated by the redirect service following the successful authorisation of the card.
PAYER_SETUP_MSG	Successful
PMT_SETUP=508	The result of the card new XML generated by the redirect service following the successful set up of the payer.
PMT_SETUP_MSG	That payment method already exists

In this instance, the merchant should expect to see the following elements returned in the response:

```
REALWALLET_CHOSEN=1
PAYER_SETUP=00
PAYER_SETUP_MSG=Successful
SAVED_PAYER_REF=pgtestpayer4
PMT_SETUP=508
PMT_SETUP_MSG= That payment method already exists
RESULT=00
```

8.6.2.3 Payer and Payment Setup Fail

RESULT=00	The result of the authorisation request
PAYER_SETUP=508	The result of the payer new XML generated by the redirect service following the successful authorisation of the card.
PAYER_SETUP_MSG	Error creating payer
PMT_SETUP=508	The result of the card new XML generated by the redirect service following the successful set up of the payer.
PMT_SETUP_MSG	Error creating payment method

In this instance, the merchant should expect to see the following elements returned in the response:

```
REALWALLET_CHOSEN=1
PAYER_SETUP=508
PAYER_SETUP_MSG= Error creating payer
PMT_SETUP=508
PMT_SETUP_MSG= Error creating payment method
RESULT=00
```

8.6.3 Transaction Unsuccessful

RESULT=101	The result of the authorisation request

In this instance, the merchant will not see any additional RealVault values returned as the RealVault process will not be attempted in a case where the card has declined.

8.7 Request Hash for RealVault Transactions

The hash string for the RealVault includes the payer and payment references.

Format:	timestamp.merchant_id.order_id.amount.currency.payerref.pmt_ref
Example:	20090320151742**.**yourmerchantid**.**transaction01**.**9999**.**EUR**.**bloggsj01.visa1

Note: The digital signature for RealVault Redirect is different than the digital signature for the standard HPP RealAuth transactions. If either of the "OFFER_SAVE_CARD" or “CARD_STORAGE_ENABLE” values is set to 1, then you have indicated you wish to use RealVault and you are required to use the digital signature outlined above. If both “CARD_STORAGE_ENABLE” and "OFFER_SAVE_CARD" values are set to 0 or not present, then you have indicated you do not wish to use RealVault and you are required to use the standard digital signature outlined in Chapter 6.

Using the details from the following example, a SHA1HASH has been constructed below:

```
<form method="POST" action="https://hpp.globaliris.com/pay">
<input type="hidden" name="MERCHANT_ID" value = “thestore">
<input type="hidden" name="ORDER_ID" value="ORD453-11">
<input type="hidden" name="ACCOUNT" value="internet">
<input type="hidden" name="AMOUNT" value="29900">
<input type="hidden" name="CURRENCY" value="EUR">
<input type="hidden" name="TIMESTAMP" value="20130814122239">
<input type="hidden" name="CARD_STORAGE_ENABLE" value="1">
<input type="hidden" name="OFFER_SAVE_CARD" value="1">
<input type="hidden" name="PAYER_REF" value="newpayer1">
<input type="hidden" name="PMT_REF" value="mycard1">
<input type="hidden" name="PAYER_EXIST" value="0">
<input type="hidden" name="SHA1HASH" value="32 character string">
<input type="hidden" name="AUTO_SETTLE_FLAG" value="1 or 0">
<input type="submit" value="Click here to Purchase">
</form>
```

Form a string by concatenating the above fields with a period (".") in the following order (TIMESTAMP.MERCHANT_ID.ORDER_ID.AMOUNT.CURRENCY.PAYER_REF.PMT_REF) Like so:

(20130814122239.thestore.ORD453-11.29900.EUR.newpayer1.mycard1)

Get the hash of this string (SHA-1 shown below).
(976c68e39a41aa48feffedf7e26ca59b225a85cd)

Create a new string by concatenating this string and your shared secret using a period.
(976c68e39a41aa48feffedf7e26ca59b225a85cd.mysecret)

Get the hash of this value. This is the value that you send to Global Iris.
(4106afc4666c6145b623089b1ad4098846badba2)

When Global Iris receives the request, we perform the same procedure on the seven pieces of information and your shared secret (which we have stored in our database). If the resulting hash is the same as the one that you sent us then the data could only have been sent by someone that had your shared secret.

9 Dynamic Currency Conversion

9.1 Overview

Dynamic Currency Conversion (DCC) is a service offered by HPP which enables you to offer international cardholders the choice of paying either in the currency of their own card or the currency that you trade in. This offers the customer an exchange rate at the point of sale rather than at the point of settlement, which is what happens if DCC is not present.

For example, say the only currency you are transacting in is Pounds Sterling (GBP). A customer then purchases an item on your website for £100. If you are not using DCC, a customer with a US Dollar (USD) must pay in GBP. It is only when they see their bank statement that they will know exactly how much they have been charged for the transaction.

12/09/2013	TOYS'R'US FIFTH AVENUE NY	$79.99
13/09/2013	**MYSHOP.IE DUBLIN IE100.00 GBP @ 1.3672 USD/GBP**	**$136.72**
15/09/2013	MACY'S 134TH STREET NY	$19.45

Further to this, it is the bank that issued the customer's credit card that controls the exchange rate that is applied to the customer.

Now, if a USD customer comes back to your website and again purchases an item worth £100, but this time your website has been enabled for DCC. Once the customer enters their card number, HPP will offer them a choice between the currency that their card was issued in, and the currency that was sent in the transaction post request. The customer will now know immediately at the point of sale exactly how much they will be charged for the transaction. Should the customer choose the USD amount, they will see the following on their bank statement:

12/09/2013	TOYS'R'US FIFTH AVENUE NY	$79.99
13/09/2013	**MYSHOP.IE DUBLIN IE**	**$129.44**
15/09/2013	MACY'S 134TH STREET NY	$19.45

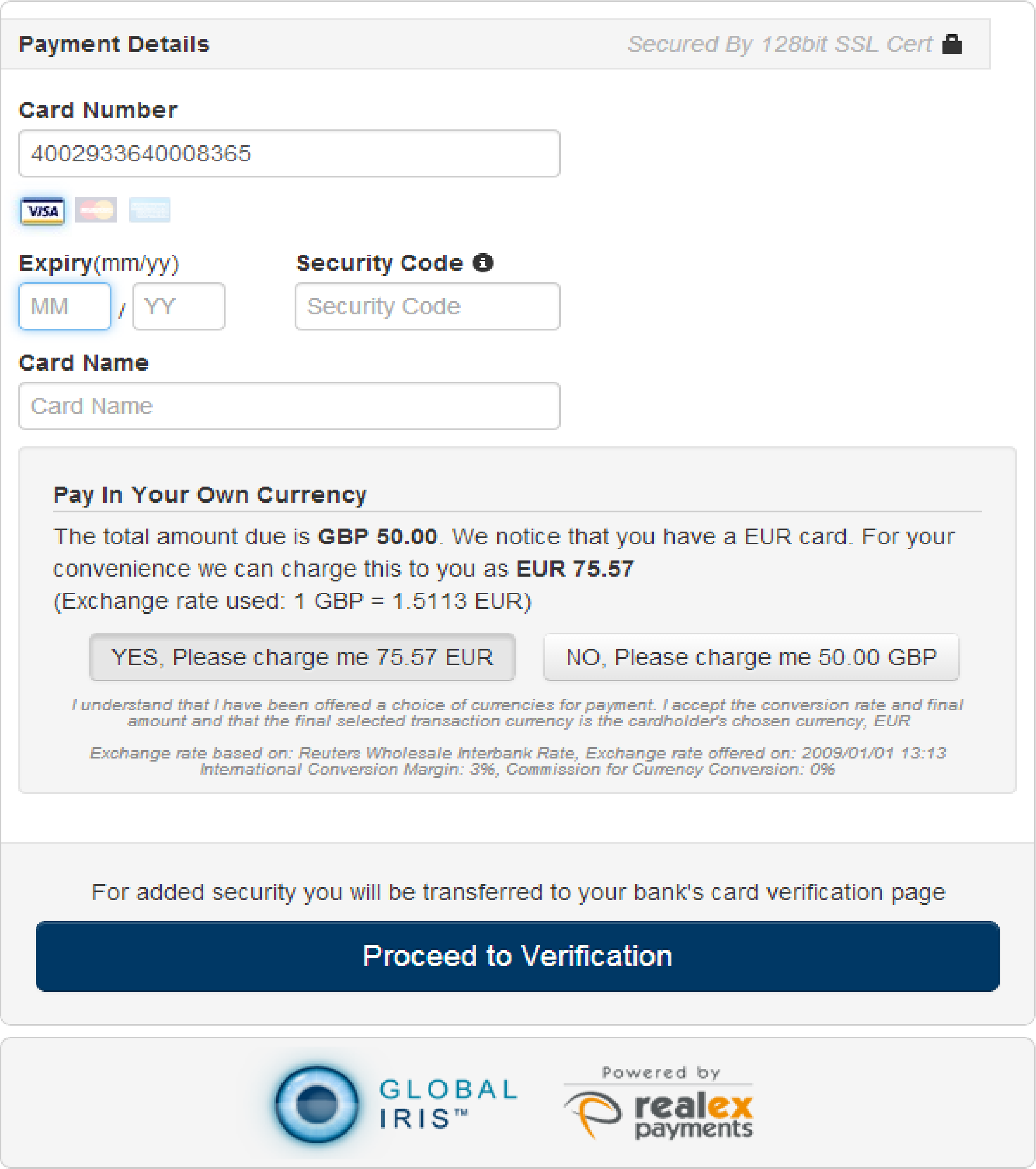
The amount charged on the customer's bank state will be exactly the same as what they were offered on your website. DCC gives cardholders choice, certainty and peace of mind when making an international transaction, which can help to reduce disputes.

Note: The ability to process DCC transactions depends on your acquiring bank. For certain acquiring banks, you will need to have an agreement in place with a Currency Conversion Processor (CCP). Your acquiring bank can assist you with this.

9.2 DCC Transaction Flow with HPP

To accept DCC transactions via HPP, there is no extra integration work to be performed on your side. However, when processing DCC transactions, you will receive extra fields in the response post sent to your response script. Your response script should be designed to handle these extra fields. This will be discussed in greater detail later in the chapter.

A customer checks out on your website as usual, and they are redirected to HPP. When the customer enters in their card number, a request is sent by HPP to your Currency Conversion Processor to see if there is an exchange rate available between the currency of the card and the original currency of the transaction. If an exchange rate is available, the cardholder is presented with the following option:



Payment Details *Secured By 128bit SSL Cert*

Card Number

4002933640008365

Expiry(mm/yy) MM / YY

Security Code Security Code

Card Name Card Name

Pay In Your Own Currency

The total amount due is **GBP 50.00**. We notice that you have a EUR card. For your convenience we can charge this to you as **EUR 75.57**
(Exchange rate used: 1 GBP = 1.5113 EUR)

YES, Please charge me 75.57 EUR | NO, Please charge me 50.00 GBP

I understand that I have been offered a choice of currencies for payment. I accept the conversion rate and final amount and that the final selected transaction currency is the cardholder's chosen currency, EUR

Exchange rate based on: Reuters Wholesale Interbank Rate, Exchange rate offered on: 2009/01/01 13:13 International Conversion Margin: 3%, Commission for Currency Conversion: 0%

For added security you will be transferred to your bank's card verification page

Proceed to Verification

In this example, the transaction has been posted to Global Iris in EUR and the cardholder has a GBP card. The cardholder is informed at the point of sale, exactly how much they will be charged in their card's currency, and also what exchange rate the transaction has been applied to the transaction. The customer can choose to accept the DCC and pay in their card's currency, or they can decline and choose to pay in the original transaction currency. Regardless of which option the cardholder chooses, you will receive the funds in your own transaction currency.

Upon clicking “Pay Now”, the transaction processes in the same manner as a standard card transaction.

9.3 Additional DCC Response Values

The only significant difference between DCC transactions and standard card transactions from an integration point of view is that additional values are posted back in the response. The additional fields are described below:

Field Title	Description
DCCCCP	The Currency Conversion Processor (CCP) used for the transaction.
DCCRATE	The exchange rate between the cardholder’s card currency and the original transaction currency that was received from the Currency Conversion Processor (CCP).
DCCMERCHANTAMOUNT	The original amount of the transaction.
DCCCARDHOLDERAMOUNT	The amount of the transaction in the cardholder’s card currency.
DCCMERCHANTCURRENCY	The original currency of the transaction.
DCCCARDHOLDERCURRENCY	The currency of the cardholder’s card.
DCCMARGINRATEPERCENTAGE	The foreign exchange margin that is applied to the transaction.
DCCEXCHANGERATESOURCENAME	The source of the exchange rate that was applied to the transaction.
DCCCOMMISSIONPERCENTAGE	For receipt printing purposes only for regulatory requirements.
DCCEXCHANGERATESOURCETIMESTAMP	The date and time that the exchange rate was offered.
DCCCHOICE	If the cardholder chooses to take the option of DCC, this will be set to “Yes”. If they don’t, it will be set to “No”.

9.4 Enabling/Disabling DCC

Should you wish to enable or disable DCC for a particular transaction, there is an optional field that can be sent in your post request to do so. The details of the field are outlined below:

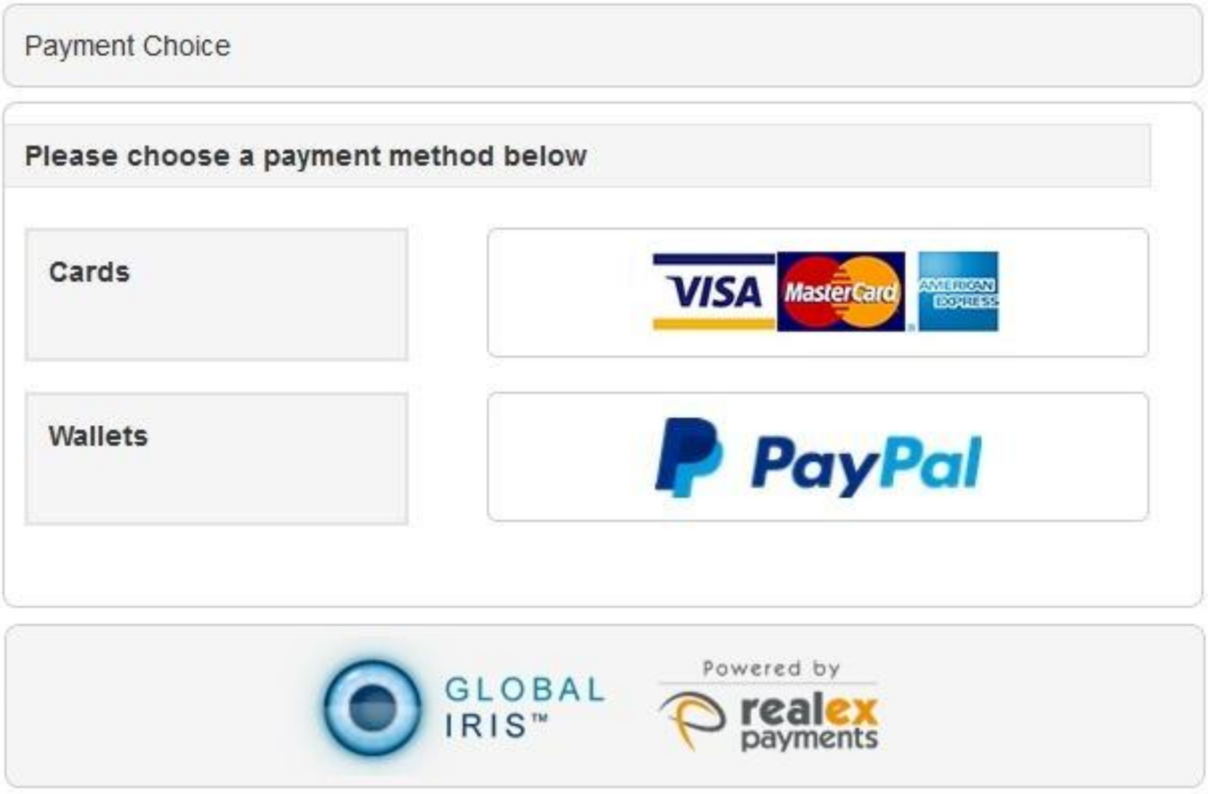
Field Title	M/O	Format	Length	Description
DCC_ENABLE	*O*	0 or 1	1	This field determines whether DCC is activated or not. If it is set to “1” then DCC is enabled, if set to “0” then it is not.

Note: If this field is not sent in, DCC will be offered based on your account setup.

10 Alternative Payment Methods

In addition to card transactions, the Hosted Payment Page gives you the ability to accept transactions from a number of other payment methods. Changes to the HPP post request and response (where applicable to the alternative payment method) are detailed in this section.

Where multiple payment methods are configured on your account, the customer will first be delivered to a payment method selection page to enable them to select their preferred payment method. You should therefore be providing the additional required and optional fields for any of your configured payment methods, since the customer may select any of the payment methods presented to them on the payment method selection page.



Payment Choice

Please choose a payment method below

<u>Note</u>: Depending on the alternative payment method which you are adding to your Global Iris Hosted Payment Page, you may have to complete third party account configuration requirements. Global Iris require specific third party account configuration details in order to configure your Global Iris merchant account accordingly. Global Iris support will provide direction on any third party configuration requirements based on the payment method which you are integrating.

10.1 Pre-Selecting Payment Methods

You have the option of either allowing the customer to select a payment method from all payment methods configured on your account, or pre-selecting one or more payment methods in the HTTP POST when you pass the transaction to Global Iris. In order to do this, include the optional “PM_METHODS” field as outlined below.

Field Title	M/O	Format	Length	Description
PM_METHODS	*O*	a-z A-Z 0-9 _ -	0-100	Optional field which allows you to select payment method(s) to offer the customer, or route customer to a specific payment method. E.g. cards, paypal, sofort, giropay, elv, ideal If you offer a specific range of payment methods you should also provide the additional required and optional fields for any of these payment methods. **Note**: Payment methods you pass through must already be configured on your account by Global Iris.

To bypass the payment method select screen and route the customer to an individual payment method (e.g. PayPal below), include the PM_METHODS field in this format in the HTTP POST:

```
<input type="hidden" name=" PM_METHODS " value="paypal">
```

To offer selected payment methods to the customer (i.e. a subset of all payment methods which are available on the subaccount), include the PM_METHODS field in this format in the HTTP POST:

```
<input type="hidden" name=" PM_METHODS " value="cards|paypal|sofort ">
```

10.2 PayPal

Additional fields can be added to the post request for PayPal transactions. You can pass transaction references and a transaction description to PayPal if required. In order to qualify for PayPal's Seller Protection, you must pass the customer’s shipping address in the post request.
The additional fields are detailed below:

```
<form method="POST" action="https://hpp.globaliris.com/pay">
<input type="hidden" name="MERCHANT_ID" value=" Global Iris
merchant-id">
<input type="hidden" name="ORDER_ID" value="unique order-id">
<input type="hidden" name="ACCOUNT" value="sub account name">
<input type="hidden" name="AMOUNT" value="amount">
<input type="hidden" name="CURRENCY" value="currency code">
<input type="hidden" name="TIMESTAMP" value="yyyymmddhhmmss">
<input type="hidden" name="SHA1HASH" value="40 character string">
<input type="hidden" name="AUTO_SETTLE_FLAG" value="1 or 0">
<input type="hidden" name="COMMENT1" value="Freeform comment field">
<input type="hidden" name="VAR_REF" value="Customer reference">
<input type="hidden" name="ADDRESS_OVERRIDE" value="1 or 0">
<input type="hidden" name="HPP_NAME" value="Ship to name">
<input type="hidden" name="HPP_STREET" value="Ship to street 1">
<input type="hidden" name="HPP_STREET2" value="Ship to street 2">
<input type="hidden" name="HPP_CITY" value="Ship to city">
```

```
<input type="hidden" name="HPP_STATE" value="Ship to state">
<input type="hidden" name="HPP_ZIP" value="Ship to zip/postal code">
<input type="hidden" name="HPP_COUNTRY" value="Ship to country code">
<input type="hidden" name="HPP_PHONE" value="Ship to phone number">
<input type="submit" value="Click here to Purchase">
</form>
```

Field Title	M/O	Format	Length	Description
ORDER_ID	*M*	a-z A-Z 0-9 _ -	1-40	A unique alphanumeric id that’s used to identify the transaction. No spaces are allowed. Note that you can pass a reference to PayPal by using this field, allowing reconciliation between Global Iris and PayPal reports.
COMMENT1	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | = ;	0-255	A freeform comment to describe the transaction. If populated for a PayPal transaction, this will be visible to the buyer on the PayPal Payment review page; this field will be visible to buyer on the PayPal payment review page.
VAR_REF	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	0-50	Any reference you also would like to assign to the customer. If populated for a PayPal transaction, this will be visible to the buyer on the PayPal Payment review page.
SHIPPING_ADDRESS_ENABLE	*O*	0 or 1	1	This field determines whether the passing of PayPal shipping address details will be activated or not. If it is set to “1” then the passing of the shipping address is enabled, if set to “0” then it is not.
ADDRESS_OVERRIDE	*O*	0 or 1	1	This field determines whether the shipping address can be changed by the customer on the PayPal review page. If it is set to “1” then the shipping address can be overwritten. If set to “0” then it cannot.
HPP_NAME	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	1-32	Ship to name.
HPP_STREET	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ /	1-100	Shipping address line 1.

Field Title	M/O	Format	Length	Description
		@ ! ? % ( ) * : £ $ & € # [ ] | =		
HPP_STREET2	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	1-100	Shipping address line 2.
HPP_CITY	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	1-40	Ship to city.
HPP_STATE	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	1-40	Ship to state.
HPP_ZIP	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	1-40	Ship to zip/postal code.
HPP_COUNTRY	*O*	A-Z	2	Ship to country code.
HPP_PHONE	*O*	a-z A-Z 0-9 ' ", + “” . _ - & \ / @ ! ? % ( ) * : £ $ & € # [ ] | =	1-20	Ship to phone number.

If the customer selects PayPal as their preferred payment method on the payment method selection page, they will be redirected to the PayPal website, where they will be asked to authenticate themselves. After entering their correct username and password, the customer can proceed in two ways:

1. Accept the transaction and click “Pay Now”. In this scenario, the transaction will be processed for payment and the customer will be redirected back to your response page on the Global Iris secure server. A post response is sent back to your response script, which is very similar to the response received for card transactions, with some minor differences. The following two fields are additional fields returned for PayPal transactions:

Field Title	Format	Length	Description
PAYMENTMETHOD	a-z A-Z 0-9	1-30	The type of payment method used, i.e. “paypal” will be returned for PayPal transactions.
PM_OPTS	-	-	Contains all other PayPal-specific information for the given transaction in the form of a JSON string.

2. Cancel the transaction. In this scenario, the transaction will not be processed. The customer will be redirected back to your response page on the Global Iris secure server and a post response will be sent to your response script. The response code posted back to your script for cancelled PayPal transactions will be 110.

An example of a post response for a successful PayPal transaction is as follows:

```
AMOUNT=5000
CURRENCY=EUR
PASREF=13764787081583009
PAYMENTMETHOD=paypal
TIMESTAMP=20130814143728
MERCHANT_ID=thestore
ACCOUNT=internet
ORDER_ID=ZZGwRHcFJGPjD5ybE85zI2npvG
SHA1HASH=b43eb70f8ec51ba7a799dd3afacb60d4c0ae5022
RESULT=00
MESSAGE=SUCCESS
PM_OPTS =
{"CoupledPaymentInfo":""}{"SuccessPageRedirectRequested":false}{"Build":8725992}{"CorrelationID":"
2e8842e84367f"}{"Token":"EC-
5MJ91664G4190730X"}{"PaymentInfo":{"ProtectionEligibilityType":"ItemNotReceivedEligible,Unauthori
zedPaymentEligible","SellerDetails":{"SecureMerchantAccountID":"FNAAD6WMVBVT6"},"ReasonCod
e":"none","GrossAmount":{"content":50,"currencyID":"EUR"},"TransactionType":"express-
checkout","PaymentDate":"2013-08-
14T14:37:28Z","TaxAmount":{"content":0,"currencyID":"EUR"},"ParentTransactionID":"","PaymentStatu
s":"Pending","ProtectionEligibility":"Eligible","PendingReason":"multi-
currency","TransactionID":"8JT05628XA900224F","PaymentType":"instant","ExchangeRate":"","Receip
tID":""}}{"Version":98}{"Timestamp":"2013-08-14T14:37:28Z"}{"Ack":"Success"}
```

Global Payments
51 De Montfort Street
Leicester
LE1 7BB
Tel 0845 702 3344*
Textphone 0845 602 4818
Email globaliris@realexpayments.com

Global Payments is HSBC's preferred supplier for card processing in the UK.

Global Payments is a trading name of GPUK LLP. GPUK LLP is authorised by the Financial Conduct Authority under the Payment Services Regulations 2009 (504290) for the provision of payment services.

GPUK LLP is a limited liability partnership registered in England number OC337146. Registered Office: 51, De Montfort Street, Leicester, LE1 7BB. The members are Global Payments U.K. Limited and Global Payments U.K. 2 Limited. Service of any documents relating to the business will be effective if served at the Registered Office.

*Lines are open between 9am – 5pm Monday to Friday excluding public holidays. To help us continually improve our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide a Textphone service on 0845 602 4818.