Hosted Payment Page (XML Redirect) Guide

Version 4.7 – March 2013

Corporate Gateway

Table of Contents

About this Guide

This guide describes the specifications for XML orders sent to WorldPay using the Hosted Payment Page (XML Redirect) service. It explains how to interpret the information WorldPay supplies to redirect a shopper to the payment pages and when directing the shopper back to the shop environment. The intended audience is the merchant's technical staff or the merchant's system integrator.

Because almost all communication between the merchant's system and the payment service is realised through predefined XML messages over the Internet using standard protocols, you will need basic XML programming skills and knowledge of HTTP(S). Furthermore it is recommended that you are familiar with the basics of the payments service, as described in our Introduction and Setup guide. Where applicable, this document refers to the related documentation with further details. WorldPay does not take responsibility for an external link's operation or content.

Update History

Version	**Change description**	**Date**
4.7	List of payment method codes and test card numbers have been updated.	March 2013
4.6	Information about alternative payment methods (supported by WorldPay AP Ltd.) has been moved to the Alternative Payment Methods Guide.	December 2012
4.5	• Updated the list of alternative payment methods and the maximum and minimum amounts. • Added information about transaction statuses returned in pendingURL.	September 2012
4.4	• Updated the list of alternative payment methods. • Added maximum and minimum amounts that are allowed on alternative payment methods. • Added information about querying payment reference and list of banks for offline bank transfers.	July 2012
4.3	Payment method code corrections.	May 2012
4.2	Test card number corrections.	April 2012
4.1	statementNarrative element added. New alternative payment method codes added.	March 2012

4.0	Gateway and guide name added to navigation path	December 2011
3.1	Payment Page update	October 2011
3.0	WorldPay rebrand	July 2011
	Global Gateway update	August 2010

Copyright

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 WorldPay Limited. WorldPay Limited, therefore, assumes 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 WorldPay. WorldPay (UK) Limited has made every effort to ensure the accuracy of this material.

Introduction

XML (Extensible Markup Language) is a text format for encoding documents electronically and is a universal way of exchanging documents and data across applications and platforms. It is used by WorldPay to send pre-defined messages containing technical information about a payment between our own payment service and a merchant's system.

Our payments service allows merchants who use the XML Hosted Payment Page (XML Redirect) model to:

- submit orders with payment details
- send a modification for the order
- perform an inquiry to request the payment status of the order

What is the Hosted Payment Page (XML Redirect) Service?

The Hosted Payment Page (also known as XML Redirect) service is an integration method to our payment service, suited for Internet shop environments, call centres or reservation centres, and multi-channel sales situations. It has been developed specifically for merchants who do not want to collect or store shopper payment details using their own system. It does this by redirecting shoppers from the merchant's web shop to the WorldPay payment pages, a secure environment where details can be entered to initiate a payment.

Our Hosted Payment Page service provides a secure and low cost solution for merchants. It allows for real-time processing of payments and provides WorldPay with the required information to perform active fraud risk assessment. It also offers the maximum number of up-to-date payment methods (some payment methods are unavailable using other connection types) and is the fastest way to get up and running with on-line payments.

Overview of the Hosted Payment Page (XML Redirect) Service

The Hosted Payment Page service requires that a merchant's system must first collect order and shopper information; and then generate an order in XML format that is delivered to the WorldPay payment service.

Upon receipt of the XML order WorldPay sends a reply to the merchant's system. The reply contains a URL required to redirect the web browser of the shopper (or operator) from the shop to the secure WorldPay environment to submit the payment details.

After the shopper has entered the payment details WorldPay redirects the shopper's browser back to the shop environment. Please note that is dependent on you providing result URLs in order to redirect shoppers to the correct result page on your website. If these are not provided then the default result page will be displayed and shoppers will not be returned to the shop environment. For further information please refer to Result URLs.

The merchant's system should be able to send and interpret the XML messages as specified in this guide, and be set-up for the required HTTP(S) connections to our payment service.

Creating an XML Order

Orders submitted to the WorldPay payment service are required to be valid XML files as specified in this guide and in the Document Type Definition (DTD) available at

```
http://dtd.worldpay.com/paymentService_v1.dtd
```

XML files are valid if they are well-formed, that is, they have a correct XML syntax, and conform to the WorldPay Document Type Definition (DTD). The content of the XML orders should always be in compliance with your contract with WorldPay and should not exceed 4k in size.

Structure of an XML Order

A typical Hosted Payment Page (XML Redirect) order contains the mandatory elements: `description, amount,` and `paymentMethodMask`. It can also contain optional elements: `orderContent` and `shopper.`

The sections listed here describe the general structure of an XML order. Please note that not all possible elements for an XML order are listed here. Refer to the WorldPay DTD for a complete overview of the possible order elements.

XML and Document Type Declaration (DTD)

As with all well-formed valid XML documents, an XML order submission begins with an XML declaration and a document type declaration, containing the root element `paymentService` and the reference to the our public payment DTD:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE paymentService PUBLIC "-//WorldPay//DTD WorldPayPaymentService
v1//EN" "http://dtd.worldpay.com/paymentService_v1.dtd">
```

Merchant and Service-specific Information

The `paymentService` root element has two required attributes: the version number of the Payment Service DTD and your merchant code. The merchant code is issued by WorldPay and is always in capitals. An example for merchant code MYMERCHANT is:

```
<paymentService version="1.4.1" merchantCode="MYMERCHANT">
  <submit>
...
  </submit>
</paymentService>
```

The `paymentService` element contains the child element `submit` to classify the XML message as a submission.

Installation, Order Description and Amount

Within the `submit` element the `order` element and its content describe the goods or services that are being ordered. The `order` element has an `orderCode` attribute whose value must be *unique*. Order codes can be up to 64 characters long; neither spaces, nor quotes nor the “<” and ”>” characters are allowed. The `order` element also includes the attribute `installationId`, which is the identification code related to your payment page customisation configuration.

Please ensure that the orderCode you supply is unique. An order with a previously used order code cannot be processed correctly.

Please note that `installationId` is only required if you have switched to the new hosted payment pages.

The first two child elements of the order element are `description` and `amount`. The `description` element should contain a simple one-line description of the order and can be up to 50 characters long. The `amount` element has the attributes: `value` (no decimal point or comma), the `currencyCode` (ISO 4217 code) and `exponent` (specifies where the decimal point or comma should be placed, counting from the right).

The amount value is the total amount the shopper is expected to pay. A list of currency codes and their respective exponents can be found in the appendix ISO Currency Codes.

```
<order orderCode="T0211010">
    <description>20 English roses from MYMERCHANT Webshop</description>
    <amount value="2600" currencyCode="GBP" exponent="2"/>
...
</order>
```

Order Content

The third child element of the order element is orderContent. You can deliver the order content in HTML format. When supplying HTML order content the only HTML tags allowed are permitted tags between the <body> and </body> tags of a valid HTML document. No form of scripting is allowed in the order content.

As a security measure we employ a list of permitted attributes (often referred to as a 'whitelist') from the Open Web Application Security Project (OWASP). Only codes that are included on the reference list will be displayed when output to a web browser. Validation of all incoming data and appropriate encoding of all output data will prevent unauthorised scripts from running in the browser. Please refer to OWASP's 'AntiSamy' Project as a guide at: https://www.owasp.org for a list of permitted tags.

The order content must be less than 10 kilobytes and should always be included in a `CDATA` section to avoid parsing problems. The order content must use the same character encoding as specified in your XML request.

```
<orderContent>
  <![CDATA[content here]]>
</orderContent>
```

Please note, it is our policy not to allow images to be inserted into HTML order content for security purposes. If you need to include images in your order content then please contact the Technical Support team, who will upload these for you.

Payment Method Mask

The fourth `order` child element is `paymentMethodMask`. It limits the available payment methods to be shown to the shopper. The `paymentMethodMask` element must have at least one `include` element that defines a single specific payment method to be included, for example: `<include code="VISA-SSL"/>,` where `VISA-SSL` is the included payment method code.

For every payment method available for your account a separate `include` element must be specified. Alternatively, to include all payment methods available, you can use one include element with the payment method code “`ALL`“. To include only on-line payment methods use the payment method code “ONLINE”.

With the optional `exclude` element you then can exclude a particular payment method from the list of payment methods, for example: `<exclude code="AMEX-SSL"/>` excludes the payment method AMEX-SSL (American Express).

A list of payment method codes can be found in the appendix Payment Method Codes.

An example of the paymentMethodMask is:

```
<paymentMethodMask>
  <include code="ALL"/>
  <exclude code="AMEX-SSL"/>
</paymentMethodMask>
```

In this example all available payment methods will be offered to the shopper, except American Express (AMEX).

You can use different payment method masks for different orders.
To bypass the payment method selection page you can specify the Preferred Payment Method. For more information see: Preferred Payment Method.

Shopper Information

The fifth order child element is `shopper` and it is used to provide extra information about the shopper in the XML order, for example the `shopperEmailAddress`. If applicable, its value can be used by WorldPay for risk assessment purposes or to send an email to the shopper when the payment is authorised or refused.

```
<shopper>
  <shopperEmailAddress>jshopper@myprovider.int</shopperEmailAddress>
</shopper>
```

Billing Address

A sixth `order` child element is `shippingAddress`. It is an optional element that enables you to pre-populate the billing address fields on the Payment Page we present to your customers.

Please note: shoppers can change the address on the payment page - it is not 'fixed' - so you cannot assume it will be the address we use to carry out fraud-screening checks such as AVS (address verification) or that it is the same as the billing address your own system / shopping cart may record for a given order.

Thus, if you pre-populate the billing address fields on the payment page with data collected on your own system and the shopper then changes that data on the payment page, your system and ours will have different address data.

Statement Narrative

Use the `statementNarrative` element to specify text that can be displayed on the shopper's statement.

This element is currently supported only by the Qiwi, AliPay and China Union pay (CUP) payment methods.

You can specify a maximum of 255 characters, though the number of characters that are displayed on a shopper's statement can vary depending on the payment method.

```
<statementNarrative>STATEMENT NARRATIVE TEXT</statementNarrative>
```

XML Validation

When creating XML documents it is good practice to check the syntax of the candidate XML document and determine whether it conforms to its schema, expressed in the DTD. We strongly recommend that you validate the XML your system creates before submitting it to our payments service. XML that does not conform to the WorldPay DTD is not accepted.

It is important that you use an industry standard XML parser for this. Do not depend on a home-made one, which may not be able to correctly interpret the messages received from WorldPay. Different XML parsers exist for various platforms, for example please refer to: http://www.xml.org. WorldPay does not take responsibility for an external link's operation or content.

Order Example

An example of a complete XML order for the Hosted Payment Page service (XML Redirect) is shown below. The order is for 20 English roses and has an order code: T0211010. The merchant is the MYMERCHANT Webshop with merchant code MYMERCHANT, the shopper is Mr. J. Shopper and the allowed payment methods are all methods except for American Express.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE paymentService PUBLIC "-//WorldPay/DTD WorldPay PaymentService
v1//EN"
"http://dtd.worldpay.com/paymentService_v1.dtd">
<paymentService version="1.4" merchantCode="MYMERCHANT">
   <submit>
        <order orderCode="T0211010">
            <description>20 English roses from MYMERCHANT
Webshop</description>
            <amount value="2600" currencyCode="GBP" exponent="2"/>
            <orderContent>
                <![CDATA[<center><table>
                      <tr><td class="one width190" align="left"
valign="top"><span style=" font-family: Arial, Helvetica, sans-serif;
font-size: 12pt; color:
                      #002469;">Product:</span>&nbsp;&nbsp;</td>
                      <tr><td class="one" align="left" valign="top"><span
style=" font-family: Arial, Helvetica, sans-serif; font-size: 12pt;
color: #002469;"><strong>Product
                      title</strong></span></td></tr>
                 </table></center>]]>
            </orderContent>
             <paymentMethodMask>
                      <include code="ALL"/>
                      <exclude code="AMEX-SSL"/>
             </paymentMethodMask>
            <shopper>
                 <shopperEmailAddress>jshopper@myprovider.int</shopperEma
ilAddress>
             </shopper>
             <shippingAddress>
                 <address>
                     <firstName>John</firstName>
                     <lastName>Shopper</lastName>
                     <address1>Shopperstreet</address1>
                     <address2>Shopperaddress2</address2>
                     <address3>Shopperaddress3</address3>
                     <postalCode>1234</postalCode>
                     <city>Shoppercity</city>
                     <state>Shopperregion</state>
                     <countryCode>NL</countryCode>
                     <telephoneNumber>0123456789</telephoneNumber>
                </address>
             </shippingAddress>
        </order>
    </submit>
</paymentService>
```

Posting An XML Order

Introduction

To submit the XML order you have to set up an HTTP(S) connection to our payments service. How you create a connection to our payments service depends on the specifications of your platform.

Setting-up the Connection

When setting up the connection, use your merchant code (always in capitals) as the login and your XML password as the password. The XML password can be set in the Profile page of the Merchant Interface (for more details, please refer to our Merchant Interface User Guide).

Please note that the Test and Production environments are separate environments and to connect successfully to either will require that the merchant code is correctly referenced in the XML Orders you send. Please also note that the XML password can differ between the Test and Production environments.

Once you have set up the connection to the WorldPay payment service, your system has to post the XML order.

Make sure the HTTP content type is “text/xml”! *It is important to check that ‘content length' is specified correctly. Not specifying the content length will not create errors, while specifying it incorrectly will.*

The URLs to post orders to are:

- Test environment:
  https://secure-test.worldpay.com/jsp/merchant/xml/paymentService.jsp
- Production/Live environment:
  https://secure.worldpay.com/jsp/merchant/xml/paymentService.jsp

Security Requirements

Global Gateway (Corporate) supports the following protocols and encryption ciphers for secure connections to our payment service:

- Protocols: Secure Socket Layer (SSL) 3.0 or higher, or Transport Layer Security (TLS) 1.0 or higher
- Ciphers: Encryption key length equal to 128 bits (MEDIUM), or larger than 128 bits (HIGH).

Whilst MEDIUM encryption ciphers are supported, we recommend you use HIGH encryption ciphers, i.e. an encryption key length LARGER than 128 bits, to guarantee transaction security. Messages encrypted with LOW encryption ciphers (smaller than 128 bits) are not supported.

Originating IP Address

The Payment Service checks incoming connections on the originating IP address, it will only accept XML where the originating IP address is registered for the merchant.

You can register multiple IP address ranges for connecting to each of the test and production environments for each merchant code.

You can edit an IP address range to connect to the test environment yourself in the Profile page of the Merchant Interface. This must be done in the Merchant Interface for the production environment (for more details, please refer to our Merchant Interface guide). The IP address to connect to the production environment can only be changed by WorldPay.

When a merchant accesses our servers we check which IP address they're trying to access us from. If the originating IP address is not within the range specified for that merchant code and environment the connection will be refused.

Sometimes a router or a firewall can mask the IP address of the originating machine and replace it with another IP address used for all outgoing IP traffic from your network. It is important that the IP address used by your network for the machines used to send the orders to the Payment Service is registered with WorldPay.

Please note that if you submit an XML order from an unregistered IP address, you will receive a notification of a security violation from our payment service. Please keep WorldPay informed of any change in IP addresses of the originating machines. To register a new IP address, please email: customeramendments@worldpay.com.

Payment Pages

Introduction

When the WorldPay payment service has received a valid order, it will send an XML response to your system. The response includes the URL to redirect the shopper to the WorldPay payment pages and has to be parsed by your system.

It is important that you use an industry standard XML parser for this. Do not depend on a home-made one, which may not be able to correctly interpret the messages received from WorldPay. Different XML parsers exist for various platforms, for example please refer to: http://www.xml.org. WorldPay does not take responsibility for an external link's operation or content.

Redirecting the Shopper to the Payment Pages

A typical XML response to an order is shown below. For example, this might be a response to the order example shown earlier.

The redirect information is contained in the `reply` element, which contains the order code to match it to the order in your back-office system.

```
<?xml version="1.0"?>
<!DOCTYPE paymentService PUBLIC "-//WorldPay/DTD WorldPay PaymentService
v1//EN"
"http://dtd.worldpay.com/paymentService_v1.dtd">
<paymentService merchantCode="MYMERCHANT" version="1.4">
  <reply>
    <orderStatus orderCode="T0211010">
      <reference id="1234567">
https://secure.worldpay.com/jsp/shopper/SelectPaymentMethod.jsp?orderKey=
MYMERCHANT^T0211010
      </reference>
    </orderStatus>
  </reply>
</paymentService>
```

The redirect URL is contained in the `reference` element. This URL must be used literally when redirecting the shopper. If the shopper needs to be redirected in the test environment the example redirect URL will be:

```
https://secure-
test.worldpay.com/jsp/shopper/SelectPaymentMethod.jsp?orderKey=MYMERCHANT
^T0211010
```

The `id` attribute of the `reference` element can be used as a payment reference if the shopper is expected to make a payment with an off-line payment method like a bank transfer or Accept Giro. In the latter case, this number (reference id) should be printed on the Accept Giros as the payment reference. If you are sending the order solely to acquire this reference id, there is no need to use the redirection URL and redirect the shopper. Shoppers who have paid for an order using an off-line payment method sometimes refer to this number instead of the order code.

How the actual redirection is performed depends on the implementation of your system.

The WorldPay payment pages do not support iFrames.

Orders received by our payment service are available for a maximum period of five days during which the shopper has to be redirected to submit the payment details.

Customising the Payment Method Selection Pages

Appending the Redirect URL

The redirect URL provided in the response from our payment service is sufficient to redirect the shopper to the payment pages.

However, you can add additional parameters to the redirect URL to customize the appearance of these pages and provide result URLs to inform the shopper of the result of the payment attempt.

All appended parameters and their values must be URL-encoded to ensure correct processing.

Many platforms have tools (built-in functions) that can automatically URL-encode information. For programming examples, please refer to:

- http://php.net/manuel/en/function.url
- http://msdn.microsoft.com/en-us/library/zttxte6w.aspx

Please note WorldPay does not take responsibility for an external link's operation or content.

The attributes listed below can be used with redirect URLs.

- Country and Language
- Body Attribute
- Font Attribute
- Result URLs
- Preferred Payment Method
- Example - with Parameters

Country and Language

The optional parameters `country` and `language` set the default country and the language of the Payment Method Selection pages. Allowed values are the two-letter ISO 3166 country code and the two-letter ISO 639-1 language code, respectively.

```
&country=GB&language=en
```

The language setting applies to the text originating from the WorldPay payments service, not to the order description and order content you supplied.

The country setting influences which of the available payment methods are presented to the shopper. Setting a country results in presenting the international credit cards and the country specific payment methods. Country and language can be specified independently from each other. For instance, you could present the payment methods for the country Netherlands in Swedish.

The shopper has the option to select a different language and country of the first Payment Method Selection page. The default position of the language and country selection boxes is at the bottom of the page, which can be changed by WorldPay on request. You can also switch the language and country selection off in the Profile page of the Merchant Interface (for more details, please refer to our Merchant Interface User Guide). It is switched on or off for *all* transactions, it cannot be done on a per transaction basis.

Body Attribute

The optional parameter `bodyAttr` sets the body attributes of the page. Allowed body attributes are anything that is valid in the `<BODY>` tag in HTML documents.

```
&bodyAttr=bgcolor%3D%22black%22
```

In this example the background colour has been set to black. Refer to external HTML documentation for more body attributes. Note that the value of the parameter is URL-encoded.

The `bodyAttr` parameter can also be used to define a background image to the Payment Method Selection pages. Please note that if you use a background image, the host of the URL of the image must have the same IP address as the order. The Payment Method Selection pages run in a secure environment. If the image resides on a non-secure environment the WorldPay HTTPS proxy should be used. This is achieved by putting the string

```
https://secure.worldpay.com/servlet/HTTPSProxy?
```

in front of the URL of the image.

Font Attribute

The parameter `fontAttr` sets the font attributes of the payment selection screen. In the example below, the font face is set to Arial and the font colour set to white. When the font indicated is not available on the shopper's system the browser's default font will be used. It is possible to define alternative fonts by separating them with a comma (for example Arial, Verdana, Helvetica).

```
&fontAttr=face%3D%22arial%22+color%3D%22white%22
```

Result URLs

The parameters `successURL` , `pendingURL`, `failureURL` and `cancelURL` set the success URL, pending URL, failure URL and cancel URL. These URLs must reside on your server and are used to provide feedback about the payment to the shopper and in reporting the payment status to your system. Examples of result URL parameter values are:

```
&successURL=http%3A%2F%2Fwww.webshops.int%2Fsuccess.asp

&pendingURL=http%3A%2F%2Fwww.webshops.int%2Fpending.php

&failureURL=http%3A%2F%2Fwww.webshops.int%2Ffailure.php

&cancelURL=http%3A%2F%2Fwww.webshops.int%2Fcancel.php
```

You can append request variables and values to these URLs, which have to be URL-encoded as well.

Refer to the later sections on Reporting Payment Results and Payment Status for more details regarding the result URLs and the Message Authenticating Code (MAC).

Preferred Payment Method

The optional parameter `preferredPaymentMethod` sets the preferred payment method. You have the possibility to pre-select the payment method for the shopper.

```
&preferredPaymentMethod=VISA-SSL
```

In this example, the payment method is VISA. A preferred payment method can be used when you only want to accept one specific payment method (for this transaction) or when you want to bypass the payment methods presented by WorldPay because the shopper has already chosen a preferred payment method in the shopping application on your server.

When you have specified a preferred payment method, the shopper does not have the possibility to select a language and country at the bottom (or at the top) of the first Payment Method Selection page.

Example - with Parameters

This example of a redirect URL displays the use of parameters:

```
https://secure.worldpay.com/jsp/shopper/SelectPaymentMethod.jsp?orderKey=
MYMERCHANT^T0211010&country=GB&language=en&successURL=http%3A%2F%2Fwww.we
bshops.int.com%2Fsuccess.asp&failureURL=http%3A%2F%2Fwww.webshops.int%2Ff
ailure.php&pendingURL=http%3A%2F%2Fwww.webshops.int%2Fpending.html&cancel
URL=http%3A%2F%2Fwww.webshops.int%2Fcancel.html&preferredPaymentMethod=VI
SA-SSL
```

For more help and advice on how to customise the look and feel of the payment page please refer to the Customising (Advanced) guide.

Testing Transactions

A number of different cases can be tested by entering the following values as the card/accountholder name in the payment page:

- REFUSED - will simulate a refused payment
- REFERRED - will simulate a refusal with the refusal reason ‘referred'
- ERROR - will simulate a payment that ends in error.

All other card/accountholder names will simulate an authorised payment.

For test purposes we have provided a set of test credit and debit card numbers: please refer to the Appendices: Test Card Numbers.

Captures and refunds can be simulated through the Merchant Interface. Use the "Capture" or "Refund" button in the Payment Details screen of an authorised or captured test payment. Alternatively, you can send an XML capture or refund order modification to the test environment.

Testing 3-D Secure Orders

In order for merchants to test their 3-D Secure implementation, we provide a test payment service. This service can be used to submit dummy XML orders. Please note that your WorldPay account must first be enabled for 3-D Secure, which can only be done by WorldPay support. We also provide a dummy card issuer site so that this part of the process can also be tested.

The value of the Cardholder's Name field on the payment pages supplied can be used to manipulate the test, as follows:

- if the Cardholder's Name is 3D then the Test environment will act as if the credit card is participating in 3-D Secure (that is, the 3-D Security Directory would respond with enrolled)
- if the Cardholder's Name is NO3D then the Test environment will act as if the credit card is not participating in 3-D Secure (that is, the Directory would respond with not-enrolled)
- with any other value for Cardholder's Name, the Test environment will act as if it is a normal e-commerce transaction (that is, no lookup with the Directory).

Please note that the value of the Cardholder's Name *element is case-sensitive. The value must be "3D" and not "3d" for the Test Environment to act as if the credit card is participating in 3-D secure.*

Using the dummy issuer site, you can also test the payer authentication response. These four options can be selected with a drop-down list:

Option1: IDENTIFIED

- a value of IDENTIFIED means the shopper's identity is successfully verified
- a value of IDENTIFIED with No XID also means the shopper's identity is successfully verified

Option 2: NOT_IDENTIFIED

- a value of NOT_IDENTIFIED means the shopper's identification could not be verified
- a value of NOT_IDENTIFIED with No XID also means the shopper's identification could not be verified

Option 3: UNKNOWN_IDENTITY

- a value of UNKNOWN_IDENTITY means that the authentication failed

Option 4: ERROR

- and any other value such as ERROR means the verification process itself failed.

Reporting Payment Results to the Shopper

Introduction

When the shopper has selected a payment method and has entered the corresponding payment details, the payment information is submitted to the WorldPay payment service. For on-line payment methods, like credit cards, WorldPay sends the payment information to the financial institutions (acquirers) for authorisation. The result of the authorisation request is reported to WorldPay on-line. This is called the payment status and can be either AUTHORISED or REFUSED. Transactions with off-line payment methods, like bank transfers, do not yet attain a payment status. Please refer to our Payment Status Definitions guide for more about these payment statuses.

The shopper must be informed about the result of the payment. Therefore WorldPay redirects the shopper's browser to a corresponding page on your system. Off-line payment methods have at that point not reached a payment status yet. The shopper must be redirected to another page on your system informing them that the order has been placed and that you will wait for the payment before shipping the merchandise.

If a shopper terminates the payment process before submitting the payment details, the order can stay in the WorldPay system without a payment status.

Redirecting the Shopper to the Result URLs

The types of payment results possible are:

- **Authorised** our payments service redirects the shopper to the `successURL` on your system where the successful authorisation of the payment is reported.
- **Pending** our payments service redirects the shopper to the `pendingURL` on your system with information that the order is placed but the payment result is not yet available (applies to off-line payment methods). For alternative payments, when a shopper is redirected to your `pendingURL`, you can view additional information about the transaction status. For more information, see Transaction Status in the pendingURL.
- **Refused** our payments service redirects the shopper to the `failureURL` on your system informs where the refused transaction is reported.
- **Cancelled** our payments service redirects the shopper to the `cancelURL` on your system informs where the cancelled transaction is reported.

Example of a redirect URL

An example of a redirect URL, or message, to redirect the shopper to the success page of the merchant is:

```
https://www.webshops.int/success.asp?orderKey=MYADMINCODE^MYMERCHANT^T021
1010
&paymentStatus=AUTHORISED&paymentAmount=2600&paymentCurrency=EUR
&mac=0083c47880f0533d773c350ee0d51cfc
```

Note that WorldPay appends a number of parameters to the URL (for details, please refer to Reporting the Payment Status. Any request variable that you appended to the result URLs is unaltered and will also be part of the above redirect message.

Also note that when a shopper cancels a payment the redirect URL will not contain the parameter paymentStatus.

Transaction Status in the pendingURL

For alternative payments, the transaction status in the pendingURL indicates the overall status of a transaction and shows the reason why a shopper has been redirected to your pendingURL. For example, the shopper can be redirected to a pendingURL of the following form:

```
http://www.merchant.com/pending.jsp?orderKey=ORD00XW01^MERCHANTXB^jsxml21
9506440&status=ERROR
```

You can use the transaction status information to manage the pending scenario appropriately, for example by allowing the shopper to retry or select another payment type if an ERROR, FAILURE, or EXPIRED status is returned.

The various transaction statuses reported by the payment method provider in the pendingURL are described in the following table.

Status	Description
OPEN	The transaction is awaiting action by the shopper. This is the result for any offline payment method.
ERROR	There was a technical problem during the transaction. Some payment method providers also return this response when a shopper has cancelled their transaction.
FAILURE	The payment has been refused. This is an uncommon response because most alternative payment methods involve pre-funding rather than real-time authorisations. Additionally, transactions are cancelled by the shopper rather than declined by a real-time authorisation.
EXPIRED	The shopper session has expired. This status is returned if the shopper initiates a transaction, but does not complete it.

HTTPS Proxy

If a shopper is redirected from the secure location on the WorldPay payment service to a non-secure location on a merchant's system, the browser likely displays a security warning that may confuse the shopper. To avoid this warning our payment service provides an HTTPS proxy showing the result URL through the existing secure connection, instead of redirecting the shopper directly. This feature is activated by default but can be switched off in the Profile page of the Merchant Interface. If you already have a secure environment in place you need not use the proxy.

The proxy does have some restrictions:

- For security reasons the feature will only work directly after a payment has been done. This means that to test the proxy functionality you will have to go through the whole payment cycle.
- The result pages should reside on the same machine (IP address) that sends the orders to our payment service.
- Pages that redirect through the 302 HTTP return code do not function in combination with the proxy.

If the result page has a redirection itself, the way to achieve this in a manner compatible with the proxy would be to use a HTTP-refresh in the Meta tag of the document: <meta http-equiv="refresh" content="0; url=somewhere.asp">. A non-W3 supported redirection method that can be used in the result URL in combination with the WorldPay proxy is:

```
<html>
  <head>
    <script language="JavaScript">
      <!--
      self.location='/redirectedfolder/thankyou.asp/;
      //-->
    </script>
  </head>
</html>
```

This method is supported but only if implemented in the way shown above. You should replace the redirection URL with the desired URL.

Informing the shopper

In addition to the online reporting through the result pages, it is possible to send email notification to the shopper with information on the payment status. This can be done by your system or the WorldPay payment service. In both cases, the shopper's email address has to be available to the respective system.

1. **Sent by merchant system**
   Your system sends an email after it receives either a signed redirect message or an automated order notification from WorldPay. Because such an email is initiated by your system, you can choose when to send it and what information is provided to the shopper. Please refer to the section Signed Redirect Message (MAC) and to our Order Notifications guide for more details.

2. **Sent by our system**
   You can have your account configured so that WorldPay sends an email to the

shopper after a successful authorisation or a refusal. To use this method, you can change the settings and the text of the actual emails through the ‘Edit Channels' functionality in the Merchant Interface. Please refer to our Merchant Interface guide for more details.

Reporting the Payment Status

Introduction

WorldPay's redirect message to the result URL contains a number of parameters, including `paymentStatus` and a digital signature, the Message Authentication Code (MAC). The MAC provides a digital signature that allows you to verify the redirect message, i.e. to ensure that the message originated from WorldPay and that it has not been modified since WorldPay signed it. After successful verification of the redirect message you can reliably use its information to update the order's payment status in your back-office system. This method applies to the payment statuses AUTHORISED and REFUSED.

It is possible to ignore the MAC, or even have this feature switched off. When switched off the redirect message contains less parameters and WorldPay advises you to use other payment status reporting tools, e.g. order notifications, to update the order's payment status in your back-office system. For more details, please refer to our Order Notifications guide.

Signed Redirect Message (MAC)

The Message Authentication Code (MAC) is created using a key-dependent one-way hash function. Calculating a hash value on the information in the redirect message alone is not sufficient, since anybody can do that if they know the hash algorithm. Therefore, a secret value (password), only known to WorldPay and the merchant, is added to the redirect parameters before the hash value is calculated. This hash value is then added to the redirect message when it is sent, but the secret value is not.

For this signed redirect message:

```
https://www.mymerchant.com/Success.jsp?orderKey=MYADMINCODE^MYMERCHANT^T0
211010
&paymentStatus=AUTHORISED&paymentAmount=1400&paymentCurrency=GBP
&mac=25eefe952a6bbd09fe1c2c09bca4fa09
```

the signature (MAC) is added to the message as a hexadecimal representation of the hash value:

```
mac=25eefe952a6bbd09fe1c2c09bca4fa09
```

Upon receipt of the signed redirect message, you can calculate the hash value in exactly the same way, by adding the secret value to the parameters of the message and applying the hash function over it. The calculated hash value should exactly match the hash value that WorldPay has added to the redirect message.

Note that when we are directing the shopper from the payment pages to the result URLs, the definition of `orderKey` *we use* `(orderKey=ADMINCODE^MERCHANTCODE^orderCode)` *is different to that used when we redirect the shopper to the Payment Method Selection pages* `(orderKey=MERCHANTCODE^orderCode)` *as described in Payment Method Selection.*

Calculating the MAC

The MAC is not calculated over the entire redirect message, but only over the sensitive data in the message. To do this, the values of these parameters in the following order are concatenated:

```
orderKey+paymentAmount+paymentCurrency+paymentStatus+[mac secret]
```

The last value is the MAC secret (password) that only WorldPay and you know. Please note that an actual redirect message can contain more variables than shown in the example, but only the above mentioned variables are included in the calculation of the MAC. Also note that the parameter `orderKey` as displayed in the redirect message is not necessarily the same as the `orderKey` as specified in the reference element of the WorldPay XML response to an order.

The concatenated message above is then fed into a MD5 hashing function, which returns a 128-bit value. The hexadecimal representation of this value must be compared with the value of the MAC provided by WorldPay in the signed redirect. WorldPay always uses lower-case hex characters.

Most development environments offer MD5 as a standard algorithm. If not, it is very likely that there is a library available to offer an MD5 implementation.

The redirect message is verified as follows. Take the variables:

```
MYADMINCODE^MYMERCHANT^T02110101400GBPAUTHORISED@p-plepie,
```

where the MAC secret is: `@p-plepie`. The hex representation of the resulting hash value is:

```
25eefe952a6bbd09fe1c2c09bca4fa09
```

This calculated MAC equals the value provided in the signed redirect message and thus guarantees that it corresponds to order code T0211010 with a successfully authorised payment for GBP 14.

Setting the MAC Secret

In order to use this functionality, you have to set the password (MAC secret) first. This can be done in the Merchant Interface, via the Profile menu.

Note: The MAC secret can contain a maximum of 20 English alphabetic characters.

For more details, please refer to the Merchant Interface User Guide.

For new merchants the MAC feature is enabled with a system-generated password. You only need to enter a new password and save the profile to be able to check the MAC in the redirect message. Having the MAC feature enabled without checking the MAC does not affect the redirection of the shopper to your result URL.

You can also disable the MAC feature via the Merchant Interface. However, this will cause the previously set password to be lost.

Note: if you disable the MAC then there is a risk that the parameters within the redirect message could have been modified.

Appendices

Payment Method Codes

You can use the `paymentMethodMask` or the `preferredPaymentMethod` variable to determine which payment method(s) the shopper will be able to choose. Codes for the payment methods can be found in the tables below.

For the full list of payment methods, see the Document Type Definition (DTD), available at: Document Type Definition (DTD) for XML Integration.

For information about alternative payment methods that are supported by WorldPay AP Ltd., see the Alternative Payment Methods Guide.

Credit Cards

Name	**Payment Method Code**	**Area**	**Remarks**
American Express SSL	AMEX-SSL	International	N/A
VISA	VISA-SSL	International	Visa Credit/Debit/Electron.
MasterCard	ECMC-SSL	International	The name **Eurocard** is no longer in use.
AirPlus	AIRPLUS-SSL	International	N/A
Aurore	AURORE-SSL	International	N/A
Carte Bancaire	CB-SSL	France	N/A
Carte Bleue	CARTEBLEUE-SSL	France	N/A
Dankort	DANKORT-SSL	Denmark	N/A
Diners	DINERS-SSL	International	N/A
Discover Card	DISCOVER-SSL	United States	N/A
GE Capital	GECAPITAL-SSL	International	N/A
Japanese Credit Bank	JCB-SSL	International	N/A
Laser Card	LASER-SSL	Ireland	N/A
PayPal	PAYPAL-EXPRESS	International	Card/Wallet
UATP	UATP-SSL	International	N/A

Online Debit Methods

Name	Payment Method Code	Area	Remarks
Elektronisches Lastschriftverfahren	ELV-SSL	Germany	N/A
Maestro	MAESTRO-SSL	International	Issue numbers and start dates are not required. Securecode must be offered to all ecommerce shoppers.
Nordea-Bank	SOLO-SSL (Fi) EBETALNING-SSL (Se)	Finland Sweden	N/A
Paybox	PAYBOX-SSL	Germany, Austria, Spain, and UK	Payment method using mobile phone.

Offline Payment Methods

Name	Payment Method Code	Area	Remarks
AcceptGiro	ACCEPTGIRO_NL-BANK	Netherlands	Merchant has to use the 'reference id' as payment reference to be printed on the accept giro forms.
Cheque	CHEQUE BANK	Belgium	For ING shoppers only. Shopper needs to have a ING Homepay account at his bank.
Cheque	CHEQUE_GB-BANK	UK	Regular cheque payments.
Commerz Bank Online Banking Web	COMLINE-BANK	Germany	N/A
Deutsche Bank 24	DB24-BANK	Germany	N/A

Direct Debit	INCASSO_NL-FAX INCASSO_DE-FAX	Netherlands and Germany	Forms must be printed, signed and sent to WorldPay.
Direct Bank Transfer Redirect Bank Transfer	TRANSFER_AT-BANK	Austria	Bank Transfer
	TRANSFER_BE-BANK	Belgium	
	TRANSFER_DK-BANK	Denmark	
	TRANSFER_FI-BANK	Finland	
	TRANSFER_FR-BANK	France	
	TRANSFER_DE-BANK	Germany	
	TRANSFER_GR-BANK	Greece	
	TRANSFER_IT-BANK	Italy	
	TRANSFER_JP-BANK	Japan	
	TRANSFER_LU-BANK	Luxembourg	
	TRANSFER_NL-BANK	Netherlands	
	TRANSFER_NO-BANK	Norway	
	TRANSFER_PL-BANK	Poland	
	TRANSFER_ES-BANK	Spain	
	TRANSFER_SE-BANK	Sweden	
	TRANSFER_CH-BANK	Switzerland	
	TRANSFER_GB-BANK	United Kingdom	

Domestic Bank Transfer	TRANSFER_NL-BANK TRANSFER_BE-BANK TRANSFER_DE-BANK TRANSFER_FI-BANK TRANSFER_FR-BANK TRANSFER_IT-BANK TRANSFER_ES-BANK TRANSFER_GB-BANK TRANSFER_SE-BANK TRANSFER_AT-BANK TRANSFER_LU-BANK TRANSFER_CH-BANK TRANSFER_DK-BANK TRANSFER_GR-BANK TRANSFER_NO-BANK TRANSFER_JP-BANK	Netherlands Belgium Germany Finland France Italy Spain UK Sweden Austria Luxemburg Switzerland Denmark Greece Norway Japan	N/A
Dresdner Bank Internet Banking	DRESDNER-BANK	Germany	N/A
Rembours / Cash on Delivery	CASH-DELIVERY	Netherlands, Germany	N/A
Signed Direct Debit	PERMANENT_SIGNED_DD	Germany, Netherlands, Spain, and USA	N/A
Unsigned Direct Debit	SINGLE_UNSIGNED_DD	Germany, Netherlands, Spain, and USA	N/A

Online Alternative Payment Methods

Name	Payment Method Code	Area	Remarks
China Union Pay	CHINAUNIONPAY-SSL	International	N/A
ENETS	ENETS-SSL	Singapore	Bank Transfer
EPS	EPS-SSL	Austria	Bank Transfer **Note**: The EPS payment method consolidates all Austrian bank transfers and replaces ELBA, POP, and NETPAY payment methods. If you are hosting your own payment page, please be aware that the new EPS page has active restrictions on redirection within an iframe or by means of a popup. If your checkout process uses either pop-ups or iframes, shoppers cannot pay on the EPS site. The active script used by EPS is available at: https://eps-routing.sparkasse.at/appl/epsSO-test/res/vpmoHfGPNsz8GwGM--/m000/jscript/routing/bankauswahl.js.
Swedbank	HANSABANK-SSL	Sweden	Bank Transfer
IDEAL	IDEAL-SSL	Dutch	Bank Transfer
KBC	KBC-BANK	German	Transfer
PAYNOVA	PAYNOVA-SSL	International	Wallet
PayPal	PAYPAL-EXPRESS	International	Ewallet

ISO Currency Codes

Please note that amounts in the orders sent to WorldPay NEVER have any decimal delimiters. Merchants should use 'exponent' instead. Exponent is the number of decimals available in the currency. Also note that currency code is always in capitals.

In the following example the amount payable by the shopper is Euro 19,82:

```
<amount value="1982" currencyCode="EUR" exponent="2"/>
```

The full ISO 4217 list can be found at: www.iso.org. WorldPay does not take responsibility for an external link's operation or content.

Country Selection - the country Parameter

The country codes used by our payment service are two-letter 'ISO 3166' standard codes.

Note that country values are always two letters in UPPER CASE; for example Germany = DE.

You can append a `country` parameter to your redirect URLs. This parameter enables pre-selection of the country (and so the payment methods shown to shoppers) for payment pages using the Hosted Payment Page (XML Redirect) service.

Shopper Selection of Country

When at our payment pages, shoppers can select a 'Country' (this then affects the range of payment methods shown).

If you have already set a default country for the payment pages (via a `country` parameter appended to the redirect URL), then this country will show as the pre-selected country in the list of countries.

If you hide the Country and Language selection boxes for all of your shoppers, then the country and language values appended to your redirect URL will fix the text and payment methods displayed on payment pages.

Note that if you supply country values that are not in the above list then the Country for the Payment Pages defaults to OTHER COUNTRY. We then show our international payment methods to the shopper.

When at our Payment pages, shoppers can currently select country codes taken from the ISO 3166 list, which can be found at: www.iso.org. WorldPay does not take responsibility for an external link's operation or content.

ISO Country Codes

The `countryCode` element is used in XML orders/communications, it is an upper-case two-letter 'ISO 3166' standard country code, as shown in the following example:

```
    ...
<address>
    <countryCode>GB</countryCode>
</address>
```

The full ISO 3166 list can be found at: www.iso.org. WorldPay does not take responsibility for an external link's operation or content.

Security Code and Address Verification Checks and Responses

You can carry out Security Code (CVC/CVV) and Address Verification (AVS) checks on an individual redirect order.

These fraud prevention tools provide a mechanism for checking the authenticity of a transaction by comparing information entered by the shopper during the payment process, with details held by the card issuer.

If applicable, results of the check can be examined, on a per order basis, by sending an XML order inquiry for each order. For more details, please refer to our Order Modifications and Order Inquiries guide. For further information about CVC/CVV fraud prevention measures, please refer to the Fraud Screening guide.

Testing

The following CVC/CVV scenarios can be tested by entering the codes listed below in the CVC field supplied in the payments pages.

1. To test CVC:

CVC2 code	**simulated situation**
Left blank	NOT SUPPLIED BY SHOPPER
111	NOT SENT TO ACQUIRER
222	NO RESPONSE FROM ACQUIRER
333	NOT CHECKED BY ACQUIRER
444	FAILED
555	APPROVED

2. To test CVC with AMEX:

CVC2 code	**simulated situation**
Left blank	NOT SUPPLIED BY SHOPPER
1111	NOT SENT TO ACQUIRER
2222	NO RESPONSE FROM ACQUIRER
3333	NOT CHECKED BY ACQUIRER
4444	FAILED
5555	UNKNOWN
6666	APPROVED

3. To test AVS (using the billing postcode address):

AVS code	**simulated situation**
Left blank	NOT SUPPLIED BY SHOPPER
1111	NOT SENT TO ACQUIRER
2222	NO RESPONSE FROM ACQUIRER
3333	NOT CHECKED BY ACQUIRER
4444	FAILED
5555	APPROVED
6666	UNKNOWN

Language Selection Codes

The language codes used by our payment service are two-letter 'ISO 639' standard codes.

ℹ *Note that language values are always two letters in lower case; for example French = "fr"*

Shopper Selection of Language

When at our payment pages, shoppers can select a 'Language' (this then affects the text shown).

If you have already set a default language for the payment pages (via a `language` parameter appended to the redirect URL), then this language will show as the pre-selected language in the list of languages.

If you hide the Country and Language selection boxes for all of your shoppers, then the `country` and `language` values appended to your redirect URL will fix the text and payment methods displayed on payment pages.

ℹ *Note that if you try to use language values that are not in the above list then the language defaults to English.*

When at our Payment pages, shoppers can currently select any language from this list.

The full ISO 639 list can be found at: www.iso.org. WorldPay does not take responsibility for an external link's operation or content.

Test Card Numbers

You can use the following card numbers to test transactions in the test environment only. When using test cards, you can specify an expiry date up to seven years in the future. The test cards do not have a card verification code and issue number.

Card Type	**Card Number**
Airplus	122000000000003
American Express	34343434343434
Cartebleue	5555555555554444
Dankort	5019717010103742
Diners	36700102000000 and 36148900647913
Discover card	6011000400000000
JCB	3528000700000000
Laser	630495060000000000 and 630490017740292441
Maestro	6759649826438453 and 6799990100000000019
Mastercard	5555555555554444 and 5454545454545454
Visa	4444333322221111, 4911830000000, and 4917610000000000
Visa Debit	4462030000000000 and 4917610000000000003
Visa Electron (UK only)	4917300800000000
Visa Purchasing	4484070000000000

Note: Visa Purchasing transactions are treated as Visa credit card transactions.

German ELV

To test German ELV payments in the test environment a correctly formatted account number (Kontonummer) and valid bank code (Bankleitzahl) should be used, for example:

Account number: 12345678
Bank code: 10000000
Bank name: Bundesbank
Bank residence: Berlin

Payment Method	**Bank Code**	**Account Number**
ELV	20030000	92441196
ELV	43050001	122108525
ELV	30070024	5929120

If you want to test ELV transactions, ensure that ELV is activated in your production environment.

XML Error Codes

The list of XML error codes is as follows:

1. Internal error, a general error
2. Parse error, invalid xml
3. Invalid number of transactions in batch
4. Security error
5. Invalid request
6. Invalid content, occurs when xml is valid but content of xml is not
7. Payment details in the order element are incorrect

For full details of our DTD refer to:

http://dtd.worldpay.com/paymentService_v1.dtd

Examples

The following are some examples for these error codes.

Error Code 1

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE paymentService PUBLIC "-//WorldPay//DTD WorldPay PaymentService
v1//EN"
"http://dtd.worldpay.om/paymentService_v1.dtd">
<paymentService version="1.4" merchantCode="MYMERCHANT">
<reply>
<error code="1"><![CDATA[Internal error]]></error>
</reply>
</paymentService>
```

It is difficult to define internal errors as they may be caused by a number of things. Internal errors have their origin within the WorldPay system itself. When a merchant gets this error it is best to retry after a short while. When a serious internal error occurs WorldPay's technical staff are informed automatically and the problem will be corrected.

Error Code 2

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE paymentService PUBLIC "-//WorldPay//DTD WorldPay PaymentService
v1//EN" "http://dtd.worldpay.com/paymentService_v1.dtd">
<paymentService version="1.4" merchantCode="MYMERCHANT">
<reply>
<error code="2"><![CDATA[Empty body in message]]></error>
</reply>
</paymentService>
```

This error indicates that the body of the XML message posted was empty. This error is also returned when the 'content length' has been set incorrectly, i.e. too few characters have been specified.

Error Code 4

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE paymentService PUBLIC "-//WorldPay//DTD WorldPay PaymentService
v1//EN" "http://dtd.worldpay.com/paymentService_v1.dtd">
<paymentService version="1.4" merchantCode="MYMERCHANT">
<reply>
<error code="4"><![CDATA[Security Violation.]]></error>
</reply>
</paymentService>
```

This error code usually indicates one of the following: (1) there is a difference between the merchant code used to set up the connection and that referred to in the XML message, (2) a connection has been attempted from an unregistered IP, or (3) the merchant is submitting to an inactive environment, usually because they have only activated the Test environment, but are attempting to submit to production.

Error Code 5

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE paymentService PUBLIC "-//WorldPay//DTD WorldPay PaymentService
v1//EN" "http://dtd.worldpay.com/paymentService_v1.dtd">
<paymentService version="1.4" merchantCode="MYMERCHANT">
<reply>
<orderStatus orderCode="12234">
<error code="5"><![CDATA[Duplicate order.]]></error>
</orderStatus>
</reply>
</paymentService>
```

Each orderCode has to be unique. In this example the merchant tried to post an order with the orderCode 123456 to our payment service. However, this order for the merchant already exists in the WorldPay database. A simple way to make orderCodes unique is to use a date/time-stamp, an incremental number or a combination of both.