Integrate with PostFinance e-Commerce
Table of contents

1. Introduction

2. Technical information page

3. Sale process

4. Link your website to the payment page
   4.1 Where to configure?
   4.2 Form parameters
   4.3 Form action

5. Security: pre-payment check
   5.1 SHA-IN signature
      5.1.1 Creating the string
   5.2 Referrer

6. Payment page look and feel
   6.1 PostFinance Responsive Payment Page template
   6.2 Adapt and upload your own customized template
      6.2.1 Hidden fields
      6.2.2 Payment zone
      6.2.3 Style sheets
   6.3 Template hosted by merchant (Dynamic template)
      6.3.1 Hidden fields
      6.3.2 Payment zone
      6.3.3 Dynamic behaviour
      6.3.4 Style sheets
6.3.5 Performance

6.4 Mobile template
6.4.1 Layout parameters
6.4.2 Template
6.4.3 Style sheets (css)
6.4.4 Example pages

6.5 Template File Manager
6.5.1 Upload template files
6.5.2 Check and manage uploaded files
6.5.3 Default merchant template
6.5.4 Integration

6.6 Template security control

6.7 Secure environment padlock

6.8 Use of payment page in iframe

7. Transaction feedback

7.1 Default reaction

7.2 Redirection depending on transaction result

7.3 Redirection with database update
7.3.1 SHA-OUT

7.4 Server-to-server feedback (post-payment)
7.4.1 Post-payment URLs
7.4.2 Timing of the request
7.4.3 Response to the customer
7.4.4 HTTP request for status changes

7.5 Feedback parameters
7.5.1 Dynamic feedback parameters
7.5.2 Variable feedback parameters
7.6 Feedback reinitialization

7.7 Confirmation emails

7.7.1 Email to the merchant

7.7.2 Email to the customer

8. Payment link via e-mail

9. Payment method selection options

9.1 Payment method selection on the merchant's site

9.1.1 How to show a specific payment method

9.1.2 How to return from the payment page to the payment method selection screen

9.2 Show a specific list of payment methods

9.3 Exclude specific payment methods

9.4 Layout of the payment methods

9.5 Window for 3-D Secure

9.5.1 3-D Secure v1.0

9.5.2 3-D Secure v2.1 (Available in TEST)

9.6 Split credit/debit cards

10. Optional fields

10.1 Operation

10.2 User field
1. Introduction

On the next pages we explain you how to integrate your website or shop with our online secure payment page.

With PostFinance e-Commerce you:

- will integrate with payment pages on the highly secured and monitored PostFinance platform
- can customise the payment page in the same look-and-feel of your own website
- don't need to have any certificates or be responsible of sensitive data
2. Technical information page

In your PostFinance account, you'll find the Technical information page via "Configuration" in the top menu.

Per setting in the Technical information page, you'll find the "i" icon to explain the particular setting.
3. Sale process

The following screenshots represent a sale process after a basic integration of your website with our system.

On your website, the customer is shown a summary page with the details of his order. He is requested to confirm this information before proceeding to the secure payment page.

The confirmation button is in fact the visible part of an "HTML form" that contains hidden fields with the payment data, and a submission action that automatically directs the customer in secure mode to a payment page on our server. The hidden fields are described in the Link your website to the payment page chapter.

On our secure payment page, the customer can choose any of the payment methods you have selected.

If the payment is done by credit card, the customer will be requested to enter his card details. The customer can confirm or cancel the payment request.
After requesting the payment from the relevant financial institution, we show the customer a page with the result of his payment.

If the payment is refused, an error message is displayed and the customer is given the option to retry: he can either choose another payment method or change the details previously entered.

A specific page on your website can also be displayed to the customer, depending on the result of the transaction. For more information, please see [Redirection depending on transaction result](https://example.com/redirect).

![Payment Result Page](https://example.com/payment-result.png)
4. Link your website to the payment page

4.1 Where to configure?

The link between your website and our e-Commerce payment page has to be established on the last page of the shopping basket on your website, in other words: the last page of your site presented to the buyer.

A form with hidden html fields containing the order data must be integrated into this last page. The block of code you need to paste into the last page of your shopping basket is shown below:

```html
<form method="post" action="https://e-payment.postfinance.ch/ncol/test/orderstandard_utf8.asp" id=form1 name=form1>

<!-- general parameters: see Form parameters -->
<input type="hidden" name="PSPID" value=""/>
<input type="hidden" name="ORDERID" value=""/>
<input type="hidden" name="AMOUNT" value=""/>
<input type="hidden" name="CURRENCY" value=""/>
<input type="hidden" name="LANGUAGE" value=""/>
<input type="hidden" name="CN" value=""/>
<input type="hidden" name="EMAIL" value=""/>
<input type="hidden" name="OWNERZIP" value=""/>
<input type="hidden" name="OWNERADDRESS" value=""/>
<input type="hidden" name="OWNERCTY" value=""/>
<input type="hidden" name="OWNERTOWN" value=""/>
<input type="hidden" name="OWNERTELNO" value=""/>

<!-- check before the payment: see Security: Check before the payment -->
<input type="hidden" name="SHASIGN" value=""/>

<!-- layout information: see Look and feel of the payment page -->
<input type="hidden" name="TITLE" value=""/>
</form>
```
4.2 Form parameters

Although strictly taken the PSPID, ORDERID, AMOUNT, CURRENCY and LANGUAGE fields are sufficient, we nevertheless strongly recommend you to also send us the customer name (CN), customer’s e-mail (EMAIL), address (OWNERADDRESS), town/city (OWNERTOWN), postcode/ZIP (OWNERZIP), country (OWNERCTY) and telephone number (OWNERTELNO), as they can be useful tools for fraud prevention.

The following table gives an overview of the hidden fields used to transmit the ‘general parameters’ to our system (additional fields are described throughout this and related documentation):

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSPID</td>
<td>Your affiliation name in our system</td>
</tr>
<tr>
<td>ORDERID</td>
<td>Your order number (merchant reference). The system checks that a payment has not been requested twice for the same order.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>AMOUNT</td>
<td>Amount to be paid, MULTIPLIED BY 100 since the format of the amount must not contain any decimals or other separators. The AMOUNT has to be assigned dynamically.</td>
</tr>
<tr>
<td>CURRENCY</td>
<td>Currency of the order</td>
</tr>
<tr>
<td></td>
<td>ISO alpha code, e.g. EUR, USD, GBP, etc.</td>
</tr>
<tr>
<td>CN</td>
<td>Customer name</td>
</tr>
<tr>
<td></td>
<td>Will be pre-initialised (but still editable) in the Customer Name field of the credit card details.</td>
</tr>
<tr>
<td>EMAIL</td>
<td>Customer email address</td>
</tr>
<tr>
<td>OWNERADDRESS</td>
<td>Customer street name and number</td>
</tr>
<tr>
<td>OWNERZIP</td>
<td>Customer postcode or ZIP code</td>
</tr>
<tr>
<td>OWNERTOWN</td>
<td>Customer town/city/...</td>
</tr>
<tr>
<td>OWNERCTY</td>
<td>Customer country</td>
</tr>
<tr>
<td>OWNERTELNO</td>
<td>Customer telephone number</td>
</tr>
</tbody>
</table>

### 4.3 Form action

```html
<form method="post" action="https://e-payment.postfinance.ch/ncol/test/orderstandard_utf8.asp" id=form1 name=form1>
```

The action of the form will be our e-Commerce system's payment processing page.

- In the TEST environment the URL for the action will be `https://e-payment.postfinance.ch/ncol/test/orderstandard_utf8.asp`
- In the PRODUCTION environment the URL for the action will be `https://e-payment.postfinance.ch/ncol/prod/orderstandard_utf8.asp`

**Change "test" to "prod"**

When you switch from your test account to your production (live) account, you must replace "test" with "prod" in the URL of the payment page.

If you forget to change the action of your form once you start in production with real orders, your transactions will be sent to the test environment and will not be sent to the acquirers/banks, meaning you won't be paid.
5. Security: pre-payment check

5.1 SHA-IN signature

To verify the data that is submitted to its system (in case of e-Commerce the hidden fields to the payment page), PostFinance requires the secure data verification method SHA. For each order, your server generates a unique character string (=digest), hashed with the SHA algorithm of your choice: SHA-1, SHA-256 or SHA-512. The SHA-IN is auto-populated by the system with a GUID. The default SHA algorithm of your PSPID is SHA-512. Please change this configuration if your system requires the SHA-1 or SHA-256 algorithm.

A similar calculation can be done after the transaction, to verify the parameters returned with the redirection URLs. We call this the SHA-OUT.

5.1.1 Creating the string

The string that will be hashed is constructed by concatenating the values of the fields sent with the order, sorted alphabetically, in the format ‘PARAMETER=value’. Each parameter with its value is followed by a passphrase. This passphrase is defined in the Technical information page of your PostFinance account, under the tab “Data and origin verification”, section “Checks for e-Commerce”. Please note that these values are all case sensitive when compiled to form the string before the hash!

Important

- All parameters that you send (and that appear in the list in List of parameters to be included in SHA-IN calculation) will be included in the string-to-hash;
- All parameter names should be in UPPERCASE (to avoid any case confusion);
- All parameters have to be arranged alphabetically. In a SHA calculation, parameters with an ID "XX" (ID with an item number higher than 10) should be in natural sort order. For example: In a list such as ITEM 1, ITEM 2, ITEM 3...ITEM 8, ITEM 9, ITEM 10, ITEM 11; ITEM 11 is placed after ITEM 10 in a natural sort order;
- Parameters that do not have a value should NOT be included in the string to hash;
- Some sorting algorithms place special characters in front of the first letter of the alphabet, while others place them at the end. If in doubt, please respect the order as displayed in the SHA-list;
- For extra safety, we request that you use different SHA passphrases in test and production.

When you hash the string composed with the SHA algorithm, a hexadecimal digest will be returned. The length of the SHA Digest is 40 characters for SHA-1, 64 for SHA-256 and 128 for SHA-512. This result should be sent to our system in your order request, using the “SHASIGN” field.

Our system will recompute the SHA string based on the received parameters and compare the merchant’s Digest with our generated Digest. If the result is not identical, the order will be declined. This check ensures the accuracy and integrity of the order data.

You can test your SHASIGN here, and you can make a test transaction with the SHA Digest calculated by our system here.

Example of a SHA-1-IN calculation (with only basic parameters)

Parameters (in alphabetical order):

- AMOUNT=1500 (15.00 x100)
- CURRENCY=EUR
- LANGUAGE=en_US
- ORDERID=1234
- PSPID=MyPSPID

SHA-IN passphrase (in Technical information):
String to hash:
AMOUNT=1500Mysecretsig1875!?CURRENCY=EURMysecretsig1875!?LANGUAGE=en_USMysecretsig1875!?ORDERID=1234Mysecretsig1875!?PSPID=MyPSPIDMysecretsig1875!?

Resulting Digest (SHA-1):
F4CC376CD7A834D997B91598FA747825A238BE0A

If the SHASIGN sent in the hidden HTML fields of the transaction doesn’t match the SHASIGN constructed at our end with the details of the order and the passphrase entered in the SHA-IN passphrase field (in the Technical information page), you will get the “unknown order/1/s” error message in the Error logs of your account (on the payment page a general error message will be displayed).

If nothing is sent in the “SHASIGN” field in the hidden HTML fields, while a passphrase is entered in the SHA-IN passphrase field (in the Technical information page) indicating you want to use an SHA signature with each transaction – you will receive the error message “unknown order/0/s”.

Following is the hidden field used to transmit the SHA signature to our system:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHASIGN</td>
<td>Unique character string for order data validation. A string hashed with the SHA-1 algorithm will always be 40 characters long.</td>
</tr>
</tbody>
</table>

5.2 Referrer

In addition to the SHA check, you can configure the so called referrer check. With this setting, our system checks the origin of the transaction request, i.e. which URL the request comes from (= the referrer). The aim is that unauthorised URLs (that are not configured in your account) won’t be able to call the payment page.

If you go to the “Data and origin verification” tab of your Technical information page, in the “Checks for e-Commerce” section you can enter one or more URLs that you want to enable to call the payment page: orderstandard.asp / orderstandard_utf8.asp.

Important

- The URL(s) must always start with http:// or https://
- You can enter the full URL or simply the domain name; the latter will result in all subdirectories and pages of that domain being accepted
- Should you have several domains, multiple URLs can be entered, e.g. http://www.mysite.com http://www.mysite.net https://www.secure.mysite.com. The URLs must be separated by a semicolon, with no spaces before or after the semicolon.
- If you perform a test transaction from our test page, please remember to enter our site’s URL as a referrer, otherwise you will receive an error.

Although the referrer allows our system to identify the origin of an order, it does not guarantee the integrity of the data. Therefore, our system requires the use of an SHA signature.

Possible errors related to the referrer are “unknown order/1/r” and “unknown order/0/r”. Go to Possible errors for more information about these errors.
6. Payment page look and feel

**LOOK & FEEL:** Build the payment page in a way that it reflects your brand and the needs of your customers at the moment of proceeding to a payment, concluding with a coherent shopping funnel and increasing your conversion. Our payment pages are composed of 2 elements:

- Static information (e.g. your logo)
- Payment detail information (e.g. order reference, fields where the customer enters his card details, etc.)

The static information originates from our system's common layout or a specific merchant template page. Our system adds the payment details dynamically for each transaction. You can customize your payment page down to applying a custom HTML and CSS to your content. All you need to do is tell us where to include the "PAYMENT ZONE" and that will take care of the payment on your page.

**SECURED HOSTING:** PostFinance proposes a secured hosting for your payment page template which allows you to remain PCI compliant.

Note: You can skip the following demo template customization section if you do not plan to customize your payment page.

6.1 PostFinance Responsive Payment Page template

Our fully responsive payment page template is the perfect and easiest solution for a multi-screen online shopping experience for your customers. It ensures you an optimized conversion on both desktop and mobile devices.

To activate the Responsive Payment Page Template from the Back Office, go to Configuration > Template > Template Selection and click "Activate" the responsive payment page.

To personalize the template by adding your logo, go to Configuration > Template > File Manager and upload your logo which you named: "logo.png".

6.2 Adapt and upload your own customized template

Begin by downloading below the PostFinance Responsive Payment Page template source file to freely customize and fit your specific brand needs. You can fully design your own template page, leaving just one area on that page to be completed by our system. You can also host your template page and files on our secure environment, which we refer to as "static template".

**Download our demo template for e-Commerce payment pages**

Feel free to try out our demo templates that support both desktop and mobile browsers. You can use them as such or easily customize them further to fit your needs. To that end you can simply open the template css files and adapt the different value to obtain your desired page.
Other than customizing the provided css files, you can also complete the HTML by adding your own header and footer information. Please see Chapter 6.2.2 for more information. For security reasons, do not apply unauthorized external data/files; all files and data must be uploaded to File Manager in order to be used.

Once completed, follow these steps to download and apply the templates for free:

1. Download the zip file.
2. From the Back Office, go to Configuration > Template > Advanced Configuration > Allow usage of static template > Yes to activate the Static templates.
3. Go to Configuration > Template > File Manager to upload the different files included in the zip file (no folder).
4. Go to Configuration > Template > Template Selection to select your preferred “Default merchant template” for e-Commerce.

Note:
- The platform supports multiple templates. You can overrule the default template for any transaction and select a specific one using the “TP” parameter in your POST request (TP=<full name of the HTML file including extension>).

Design your own payment page.

Other than customizing the provided css files, you can also complete the HTML by adding your own header and footer information. Please see Chapter 6.2.2 for more information. For security reasons, do not apply unauthorized external data/files; all files and data must be uploaded to File Manager in order to be used.

6.2.1 Hidden fields

The following hidden field is used to transmit the file name of your template page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP</td>
<td>File name of the template hosted by PostFinance.</td>
</tr>
</tbody>
</table>

Example:

```html
<input type="hidden" name="TP" value="mytemplatefile.html">
```

6.2.2 Payment zone

The template page can be designed completely to your liking. The only requirement is that it must contain the string "$$PAYMENT ZONE$$" indicating the location where our e-Commerce module can add its fields dynamically. It must therefore contain at least the following:

```html
$$PAYMENT ZONE$$
</html>
```

Important
Do not use BASE tags, frames or FORM tags to encapsulate the $$PAYMENT ZONE$$ string.

6.2.3 Style sheets

You can personalise the look and feel of your payment pages by adding style sheets to your template page.

We have defined a class for the various types of tables and cells within our tables as well as a class for the submit buttons.

You need to add the following block of code between the tags `<head>` and `<head>` and change the properties of those classes to fit to the look
When you enter your own layout instructions, you must adhere to the cascading style sheet syntax. We strongly advise you to test it in various browsers, as the way they handle style may differ enormously.
6.3 Template hosted by merchant (Dynamic template)

The dynamic template page allows you to customise the design of the payment pages in a more advanced way than the static template does.

When you use a dynamic template page, you fully design your own template page, leaving just one area in that page to be completed by our system. The URL of your template page needs to be sent to us in the hidden fields for each transaction.

Please bear in mind that using a dynamic template page involves an additional request from our system to look up your template page. This increases the time needed for the payment process.

**Important**

To comply with the latest PCI-DSS you are required to host your template (and related files) in an environment with the highest PCI certification.

6.3.1 Hidden fields

The following hidden field is used to transmit the URL of your template page:

```html
<input type="hidden" name="TP" value="">
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP</td>
<td>URL of the merchant’s dynamic template page. The URL must be absolute (contain the full path), it cannot be relative. Do not specify any ports in your URL, we only accept ports 443 and 80. Any component included in the template page must also have an absolute URL.</td>
</tr>
</tbody>
</table>

6.3.2 Payment zone

The template page can be designed completely to your liking. The only requirement is that it must contain the string "$$PAYMENT ZONE$$" indicating the location where our e-Commerce module can add its fields dynamically. It must therefore contain at least the following:

```html
<html>
$$PAYMENT ZONE$$
</html>
```
An example of a dynamic template page is available at the following address: https://e-payment.postfinance.ch/ncol/template_standard.htm

6.3.3 Dynamic behaviour

The same template page can be used for all orders, or it may be generated dynamically by the merchant’s application according to the order parameters.

To generate the template page dynamically, the merchant can choose between creating a specific page for the order, whose URL is transmitted in the hidden fields, or using a fixed URL but returning a result derived from the order number. To allow this, our system adds the main payment data – including the merchant’s order reference number – when it retrieves the template page:

HTTP request = url_page_template ?ORDERID=...&AMOUNT=...&CURRENCY=...

6.3.4 Style sheets

You can personalise the look and feel of your payment pages by adding style sheets to your template page.

We have defined a class for the various types of tables and cells within our tables as well as a class for the submit buttons.

You need to add the following block of code between the tags <head></head> and change the properties of those classes to fit to the look and feel of your site:

```
<style type="text/css">

/*
   td.ncolh1 {background-color : #006600; color : yellow; font-family : verdana}
   td.ncoltxtl {background-color : #ffffff; color : black; text-align : right; font-weight : bold}
   td.ncoltxtl2 {background-color : #ffffff; color : black; text-align : right; font-weight : bold}
   td.ncoltxtc {background-color : #ffffff; color : black; text-align : center; font-weight : bold}
   td.ncolinput {background-color : #ffffff; color : black}
   td.ncolline1 {background-color : #ffffff; color : black}
   td.ncolline2 {background-color : #ffffff; color : black}
   input.ncol {background-color : #006600; color : white}
   td.ncollogoc {background-color : #ffffff; color : black; text-align : center; font-weight : bold}
   table.ncoltable1 { background-color: #ffffff; }
   table.ncoltable2 { background-color: #ffffff; border-width : medium; border-color : green; }
   table.ncoltable3 { background-color: #ffffff; }
 */

</style>
```

When you enter your own layout instructions, you must adhere to the cascading style sheet syntax. We strongly advise you to test it in various browsers, as the way they handle style may differ enormously.
6.3.5 Performance

Our system is configured with a 5-second time-out for the request to retrieve the merchant's dynamic template page.

Please contact our customer care MerchAndHelp, Tel. +41 (0)848 38 24 23, e-mail: merchandhelp@postfinance.ch, to change this time-out.

If a time-out occurs, our system will use the merchant's static template instead.

If no static template is configured, our system will use the PostFinance default layout as a last resort.

The configured time-out has an impact on both dynamic template requests and post-payment feedback requests (see [Direct feedback requests (Post-payment)]). Consequently, if the merchant were to change it to e.g. 15 seconds, the feedback request timeout will also increase to 15 seconds.

For each order, our system performs a request to retrieve your dynamic template page. If you have high transaction volumes or a large
template page (e.g. your dynamic template page contains a large number of images), these HTTP requests could take a bit longer. Please contact our customer care Merchanthelp for a solution if you have high transaction volumes.

6.4 Mobile template

You can optimize the display of the payment page on mobile devices (smartphones, tablets etc.) by applying a template page, enriched with style sheets, as explained in the next chapters.

6.4.1 Layout parameters

Below are the fields which can be customised by providing details in a request:

```html
<input type="hidden" name="TITLE" value="">
<input type="hidden" name="BGCOLOR" value="">
<input type="hidden" name="TXTCOLOR" value="">
<input type="hidden" name="TBLBGCOLOR" value="">
<input type="hidden" name="TBLTXTCOLOR" value="">
<input type="hidden" name="BUTTONBGCOLOR" value="">
<input type="hidden" name="BUTTONTXTCOLOR" value="">
<input type="hidden" name="LOGO" value="">
<input type="hidden" name="FONTTYPE" value="">
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TITLE</td>
<td>Title of the page</td>
<td>Title</td>
</tr>
<tr>
<td>BGCOLOR</td>
<td>Background colour</td>
<td>white</td>
</tr>
<tr>
<td>TXTCOLOR</td>
<td>Text colour</td>
<td>black</td>
</tr>
<tr>
<td>TBLBGCOLOR</td>
<td>Background colour for the right columns</td>
<td>white</td>
</tr>
<tr>
<td>TBLTXTCOLOR</td>
<td>Text colour for the right columns</td>
<td>black</td>
</tr>
<tr>
<td>BUTTONBGCOLOR</td>
<td>Button background colour</td>
<td>n/a</td>
</tr>
<tr>
<td>BUTTONTXTCOLOR</td>
<td>Button text colour</td>
<td>black</td>
</tr>
<tr>
<td>LOGO</td>
<td>URL/filename of the logo you want to display on the payment page</td>
<td><a href="https://e-payment.postfinance.ch/images/merchant/%5BPSPID%5D/%5Bimmagine">https://e-payment.postfinance.ch/images/merchant/[PSPID]/[immagine</a>]</td>
</tr>
<tr>
<td>FONTTYPE</td>
<td>Font family</td>
<td>Verdana</td>
</tr>
</tbody>
</table>

6.4.2 Template

The following hidden field is used to transmit the URL of your template page:

```html
<input type="hidden" name="TP" value="">
```
### Field Description

| TP | URL of the dynamic template page. The URL must be absolute (contain the full path), it cannot be relative. Any component included in the template page must also have an absolute URL.  

**Important:** To comply with the latest PCI-DSS (2015), you are required to host the template items used for the payment page in an environment with the highest PCI certification. Therefore, we recommend you to host your files with PostFinance.

---

**Payment zone**

The template page can be designed completely to your liking. The only requirement is that it must contain the string "$$\text{PAYMENT ZONE}$$" indicating the location where our e-Commerce module can add its fields dynamically. It must therefore contain at least the following:

```html
$$\text{PAYMENT ZONE}$$
</html>
```

Go to [Example templates](#) to get some inspiration with the templates we've created, or simply create your own template based on ours.

---

### 6.4.3 Style sheets (css)

For ease of managing and understanding of CSS we divided the template CSS into four main parts:

- **Header**
- **Payment detail**
- **Footer**
- **Payment status section**

**Note:** Although the example images below do reflect which elements will be affected by the css, the style (colours, images etc.) used may differ from what's described in the accompanying example codes.

---

**Header**

Using this style you can modify the header part of the payment page as shown below:
Payment detail

Using this style you can customise the Payment Details section as shown below:
Using this style you can set the footer part of the payment page:

```javascript
Footer
```

Element(s)

td.ncollogo
{
  text-align: center;
  font-weight: normal;
  font-size: 14px;
  padding: 2px;
  vertical-align: top !important;
}
td.ncollogo IMG
{
  width: 90px;
  height: 55px;
  margin-right: 4px;
}
Payment Status Section

Using this section you can customise the look and feel of the payment status page as shown here:

Element(s)

```
<td class="ncoltxtc">
  <h3>Your payment is accepted</h3>
  <small>Payment reference: 3001581880</small>
</td>
```
6.4.4 Example pages

Integrate with PostFinance e-Commerce
To get you started, we’ve created two pages ourselves.

The first one is a branded version which you can use as an example:

https://e-payment.postfinance.ch/ncol/StandardMobileTemplate.htm

You can also use the "stripped" version hereafter as a base to create your own template:

https://e-payment.postfinance.ch/ncol/StandardMobileTemplate_generic.htm

The same two templates with additional files (fonts, images) are available in a downloadable zip here.

6.5 Template File Manager

With the Template File Manager you can easily manage your templates and the various files that come with it.

To start using File Manager, log on to your PostFinance account and go to "Configuration" > "Template" > "File Manager".

**Important**

It's not possible to simultaneously use files previously uploaded by PostFinance and files uploaded with File Manager in your integration.

Therefore, if you have files that were uploaded by PostFinance in the past, please make sure to upload those files again yourself, using File Manager.

6.5.1 Upload template files

Under "Upload Template Files", select the "Files..." button to browse for the files you wish to upload. You can upload Javascripts, html, css and images (.css, .jpg, .jpeg, .gif, .png, .html, .js), with a maximum of 7 MB per file, and 10 MB in total.

Make your selection and then confirm.

6.5.2 Check and manage uploaded files

After the upload is done, you’ll see your uploaded files on the same page in the "Uploaded files" section.

The files will first have the “Validating” status, during which some necessary security/virus checks are being performed.

You can use the files once its status has changed to “Validated”.

Click the refresh button to check the current status of your files / click the delete button to delete the file permanently.
A file will get the “Refused” status if it didn’t pass the security check. This can be due to a virus or if the extension of the file is wrong for instance.

6.5.3 Default merchant template

Under Default settings > Default merchant template, you can configure the template you want to apply on the e-Commerce hosted payment page.

If you don’t select a default template, the platform’s default template is used.

6.5.4 Integration

In your templates you refer to your uploaded files with a code following this structure: $$$TP RESOURCES URL$$(your file name).

Note: If you want to use a resource in a CSS file, you should reference the following code: "./[your file name] instead.

Example:

```html
<html>
  <head>
    <title>Great Shop Test Page</title>
    <link rel="stylesheet" type="text/css" href="$$TP RESOURCES URL$$/layer_styling_v5.css">
    <script src="$$TP RESOURCES URL$$/test.js"></script>
  </head>
  <body>
    <div>Great Shop Template</div>
    <div>$$PAYMENT ZONES$$</div>
    <img src="$$TP RESOURCES URL$$/4ec6d9b0-2af4-4279-bfde-7fe40dfaf9e6_6.jpg" />
  </body>
</html>
```
To refer to your uploaded template in your e-Commerce integration, you send the template file name with the "TP" parameter.

Example: TP=mytemplatefile.html

When you have a basic e-Commerce integration using a logo on top of the page, you need to refer to the uploaded logo by sending the filename along with the "LOGO" parameter.

Example: LOGO=mycompanylogo.png

6.6 Template security control

To protect your customers against fraudulent activities, such as the manipulation of sensitive card data (card number, CVC), different security checks for the merchant template were made available.

In your Technical information page > Global security parameters tab > Template section, the following settings can be configured:

- **Enable Javascript check on template**
  You can enable this feature to detect Javascript usage on the template page. If Javascript is detected, the template will be blocked and the default template will be used instead.

- **Allow usage of dynamic template (optional, depending on your subscription)**
  If you select "Allow usage of dynamic template", you must configure the Trusted website host name hosting the dynamic template field. This field can contain multiple web hosts, separated by semicolons, but they should all contain the full URL, e.g. http://www.website.com/. The sub-directories can be left out, so if the dynamic template is http://www.website.com/templates/nl/template1.htm, it suffices to configure http://www.website.com as trusted web host.

  Additionally you can also configure one or more fully trusted dynamic template urls, separated by semicolons, in the Trusted dynamic template url field.

If a dynamic template is submitted with a transaction, but dynamic templates are not allowed, then the template will be blocked and our system will use the static template instead.

If there is no static template configured, then the default PostFinance template will be used. By default, "Enable JavaScript check on template" are enabled.

6.7 Secure environment padlock

The URL used to connect the customer to our platform uses a secure protocol (https). All the communication between our e-Commerce platform and the customer is securely encrypted.

However, the small padlock on the browser – which indicates to the customer that the site is secure – may not be displayed if some elements (e.g. images) in the template page are not located on a secure server or if some frames on the screen show pages that do not originate from secure sites.

Even if the payment processing communication is encrypted, most browsers will not recognise a secure connection unless all the elements on the screen, including images, sounds, etc. come from secure sites.

For merchants who do not have a secure site, please bear in mind the following rules:

1. Do not use frames for the payment pages: you can refresh the entire screen with a template page that looks as if you are using frames or allow the payment to be processed in a new window.
2. Do not link files to the template page (<link> tag) that you use for the payment page. Instead, use the <style> and <script> tags to include styles and scripts into the template page.
3. Make sure the images in your template are stored on a secure server (the template page can be on a non-secure server, however the images cannot). We offer hosting for these elements (see the image hosting options in your account).
6.8 Use of payment page in iframe

Iframes allow you to integrate an external web page (such as the payment page) on your website, while maintaining your own URL in the browser.

However, in the current context iframe also has very significant drawbacks:

- Since the URL is the merchant’s URL, it could be a simple http (instead of an https) and the padlock icon may not appear in the browser. This could cause customers to doubt the security of the webshop.
- Some payment methods (such as PayPal, Giropay, Sofort and Bancontact/Mister Cash) use redirections, which may give poor layout results and/or navigation misbehaviour.

As a result, PostFinance discourages the use of iframe, and the usage thereof is your responsibility. PostFinance strongly encourages the use of a Dynamic Template instead.

If you still wish to pursue the integration of iframe, we strongly recommend the following:

- Use iframe only on the payment method selection page (and beyond)
- Use pop-ups for external payment methods whenever possible, to ensure the visibility of third-party web applications.
7. Transaction feedback

After a transaction is processed, depending on the result, a response can be sent to your system and to the customer. Hereafter we explain how and when the transaction feedback can be sent, and what you need to set up and configure on your end to make each feedback process work.

Best practice

Redirection with parameters on the accept-/exception-/cancel-/declineurl (Redirection with database update) with a deferred post-payment feedback request as a backup (Server-to-server feedback (post-payment)).

In your PostFinance account, go to "Configuration" > "Technical information" > "Transaction feedback". Configure the settings as described below:

HTTP redirection in the browser:

Direct HTTP server-to-server request: Always deferred:

7.1 Default reaction

By default, meaning if you haven't configured Transaction feedback settings, our system will display a standard message to the customer: "Your payment is authorised" or "The transaction has been denied".
In this page, we also add a link to your website and/or to your catalogue. Usually, these links are configured in your PostFinance account’s Administrative details, which is where our system will fetch them. However, you can also override these URLs by submitting the HOMEURL and CATALOGURL fields with the other the hidden fields in the order form:

```html
<input type="hidden" name="CATALOGURL" value=""/>
<input type="hidden" name="HOMEURL" value=""/>
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATALOGURL</td>
<td>(Absolute) URL of your catalogue. When the transaction has been processed, your customer is requested to return to this URL via a button.</td>
</tr>
<tr>
<td>HOMEURL</td>
<td>(Absolute) URL of your home page. When the transaction has been processed, your customer is requested to return to this URL via a button. When you send the value “NONE”, the button leading back to the merchant’s site will be hidden.</td>
</tr>
</tbody>
</table>

### 7.2 Redirection depending on transaction result

There are four URLs which our system can redirect the customer to after a transaction, depending on the result. These are "ACCEPTURL", "EXCEPTIONURL", "CANCELURL" and "DECLINEURL".

The URLs can be configured or submitted as follows:

- Configuration in your PostFinance account: In the Transaction feedback tab of your Technical information page: "HTTP redirection in the browser"
• Submission of the URLs in the hidden fields of the order form:

```html
<input type="hidden" name="ACCEPTURL" value=""/>
<input type="hidden" name="DECLINEURL" value=""/>
<input type="hidden" name="EXCEPTIONURL" value=""/>
<input type="hidden" name="CANCELURL" value=""/>
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCEPTURL</td>
<td>URL of the web page to display to the customer when the payment has been authorised (status 5), stored (status 4), accepted (status 9) or is waiting to be accepted (pending status 41, 51 or 91).</td>
</tr>
<tr>
<td>DECLINEURL</td>
<td>URL of the web page to show the customer when the acquirer declines the authorisation (status 2 or 93) more than the maximum permissible number of times.</td>
</tr>
<tr>
<td>EXCEPTIONURL</td>
<td>URL of the web page to display to the customer when the payment result is uncertain (status 52 or 92). If this field is empty, the customer will be redirected to the ACCEPTURL instead.</td>
</tr>
<tr>
<td>CANCELURL</td>
<td>URL of the web page to display to the customer when he cancels the payment (status 1). If this field is empty, the customer will be redirected to the DECLINEURL instead.</td>
</tr>
</tbody>
</table>

### Browser alert notification: secure to non-secure environment

When a customer returns from our secure payment pages to the merchant's (your) website, he might get a browser alert warning him that he is entering a non-secure environment, as most likely he is moving from an https:// environment to an http:// environment.

When we detect a redirection to your website, we can display a message to notify the customer about the possibility of a risk, thereby avoiding any undue concern about a browser alert. You can activate this option in the Transaction feedback tab of your Technical information page, "HTTP redirection in the browser" section: "I want PostFinance to display a short text to the customer on the secure payment page if a redirection to my website is detected immediately after the payment process".

### 7.3 Redirection with database update

You can use the redirection on the redirection URLs to trigger automatic back-office tasks such as database updates. When a transaction is executed, we can send the transaction parameters on your redirection URLs.

To use this functionality, you must activate this option in the Transaction feedback tab of your Technical information page, "HTTP redirection in the browser":

- "I would like to receive transaction feedback parameters on the redirection URLs".

#### 7.3.1 SHA-OUT

The redirection is done via the customer’s browser, which makes it visible. Therefore, you must use an SHA-OUT signature to verify the contents of the request and prevent customers tampering with the data in the URL field, which could result in fraudulent database updates.

If you don't configure a SHA-OUT signature, we won't send any parameters on your redirection URLs.

The string to hash is constructed by concatenating the values of the fields sent with the order (sorted alphabetically, in the format ‘parameter=value’), followed by a passphrase. The passphrase is defined in the Transaction feedback tab of your Technical information page, "All transaction Submission modes" section.
For the full list of parameters to include in the SHA Digest, please refer to the SHA-OUT Parameter list. Please note that these values are all case sensitive.

**Important**

- All sent parameters (that appear in the SHA-OUT Parameter list), will be included in the string to hash.
- All parameters need to be sorted alphabetically
- Parameters that do not have a value should NOT be included in the string to hash
- Even though some parameters are (partially) returned in lower case by our system, for the SHA-OUT calculation each parameter must be put in upper case.
- When you choose to transfer your test account to production via the link in the back-office menu, a random SHA-OUT passphrase will be automatically configured in your production account.
- For extra safety, we request that you use different SHA passphrases for TEST and PROD. Please note that if they are found to be identical, your TEST passphrase will be changed by our system (you will of course be notified).

In the same way we recreate the Digest to validate the transaction input with the SHA-IN, you have to reconstruct the hash, this time using your SHA-OUT passphrase and the parameters received from our system.

If the outcome is not identical, the request's parameters might have been tampered with. This check guarantees the accuracy and integrity of the parameter values sent in the request.

**Example of a basic SHA-1-OUT calculation**

Parameters (in alphabetical order, as returned by PostFinance):

- ACCEPTANCE: 1234
- amount: 15
- BRAND: VISA
- CARDNO: XXXXXXXXXXXX1111
- currency: EUR
- NCERROR: 0
- orderID: 12
- PAYID: 32100123
- PM: CreditCard
- STATUS: 9

SHA-OUT passphrase (in Technical information):
7.4 Server-to-server feedback (post-payment)

After the transaction is processed, our system can send an http request transmitting the transaction data, to a URL you've specified. This process, which we often refer to as the "post-sale" request, allows you to update your database with the order status, etc. and trigger an "end of order" process (if this has not already been done after a redirection). It is also an alternative way of generating a personal response for the customer in case of specific needs (if this has not already been done via a redirection).

The set of feedback parameters is the same as that for the redirection. You can find them on the "Feedback parameters" page.

7.4.1 Post-payment URLs

You can define the URLs of two executable pages on your site in the "Transaction feedback" tab, "Direct HTTP server-to-server request" section (URL fields) of your Technical information page:

- The first field will ideally contain the URL to which the request parameters are sent if the payment’s status is accepted, pending or uncertain.
- The second field can be the URL to which the request parameters are sent when the transaction has been cancelled by the client or declined too many times by the acquirer (i.e. more than the maximum allowed number of payment attempts as set in the "Global transaction parameters" tab, "Payment retry" section of the Technical information page).

You can enter two different URLs, but you can also use twice the same. You may also enter a URL just in the first field but not for the second.

Do not specify any ports in your URL; we only accept port 443 and port 80.

Variable post-payment URLs for multiple shops

If you have a post-payment page configured in the Technical information page in your account, but you have several shops each connected to a specific directory for receiving the post-payment feedback, part of your post-payment URL can be variable.

This variable part can also be used to e.g. "adapt" the feedback request to include session information, passing it as a part of the URL.
rather than as an additional parameter. This is the case for Intershop platforms or Servlet systems.

The following hidden field should be used:

```html
<input type="hidden" name="PARAMVAR" value=""/>
```

Example:

Post-payment URL in your Technical information page:

https://www.yourwebsite.com/<PARAMVAR>/yourpage.asp

Extra hidden field sent in your order form:

```html
<input type="hidden" name="PARAMVAR" value="shop1"/>
```

Resulting in the following Post-payment URL for the transaction:

https://www.yourwebsite.com/shop1/yourpage.asp

Important: do not use any special characters in the PARAMVAR field, as they will be URL encoded, which could create invalid links.

### 7.4.2 Timing of the request

Where you configure the post-payment URLs, you must also choose the timing of the feedback request:

- **No request**

  In this case, our system will not send any feedback request. This option allows you to disable your post-payment URLs in the event of maintenance or problems on your server. You shouldn't select "No request" as you're obliged to receive post-sale requests (see Transaction Feedback to the Customer and the Merchant).

- **Always deferred (not immediately after the payment)**

  The feedback request will be sent shortly after the end of the payment process. The feedback request will be a background task and cannot be used to send a personalised feedback to the customer on your website.

  If you don't use your post-payment page to personalise a response for your customers, you can receive the feedback request in the background and deferred.

- **Always online (immediately after the payment, to allow customisation of the response seen by the customer)**

  The feedback request will be sent “online” sometime between our system’s receipt of the acquirer’s response and the time it notifies the customer of the payment result.

  In this case, the payment process takes longer for the customer, but you can send a personalised response to the customer.

  The disadvantage of the online post-payment feedback process is that your system might be detrimentally affected if there are too many requests to your post-payment page (e.g. high per-minute transaction volume) – this could result in long response times before customers receive on-screen feedback.

  This option allows merchants who require online post-payment feedback (to tailor the response displayed to the customer) to have a fall-back option, should the online request on his post-payment page fail. In this case we will retry the feedback request every 10 minutes up to a maximum of four times (deferred). In this way, you don’t miss out on the transaction feedback, should the online post-payment feedback request fail, e.g. as a result of temporary server problems at your end. The customer will be displayed the standard transaction feedback from our system (see Default reaction).

- **Online but switch to a deferred request in intervals when the online requests fail**

  This option allows merchants who require online post-payment feedback to have a fall-back option, should the online request on his post-payment page fail. In this case we will retry the feedback request every 10 minutes up to a maximum of four times (deferred). In this way, you don’t miss out on the transaction feedback, should the online post-payment feedback request fail, e.g. as a result of temporary server problems at your end. The customer will be displayed the standard transaction feedback from our system (see Default reaction).

### 7.4.3 Response to the customer

We use a possible reply from your post-payment page to show a feedback (end of transaction page) to your customer.
If your post-payment page replies with: an HTML page (containing an `<html>` tag) or a redirection (HTTP 302 Object Moved), our system will send this HTML page “as is” to the client browser or perform the redirection, rather than redirecting your customer at the end of your post-payment feedback process to one of the four URLs you may have sent in the hidden fields (ACCEPTURL, EXCEPTIONURL, CANCELURL and DECLINEURL as described in the Redirection depending on transaction result chapter).

Alternatively, if you use none of the above as feedback to your customer, you can have your post-payment page respond with a few lines of text (no `<html>` tag) which we will include in our standard response, or our system will simply show the standard response (as described in: Default reaction).

The diagram below shows the process at the end of a transaction, should the payment be authorised or accepted, with an online post-payment request. (When the payment is cancelled, declined or uncertain the process is similar but the "CANCELURL", "DECLINEURL", "EXCEPTIONURL" and "cancellation/rejection" pages are used instead).

7.4.4 HTTP request for status changes

You can also receive an HTTP request in the case of a transaction status change. Therefore, you need to enter a URL in the "HTTP request for status changes" field in the "Transaction feedback" tab of your Technical information page (and select the timing for the request).

This is similar to the post-payment feedback, with the difference that it is only relevant for potential background processes.

You can use the same URL as the one set in the "Direct HTTP server-to-server request" section.

**Note:** This "status change" URL cannot be used to generate a personal response for the customer.

7.5 Feedback parameters

When a transaction is executed, we can send the following parameter list to your redirection URLs and/or post-payment feedback URLs.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCEPTANCE</td>
<td>Acceptance code returned by the acquirer</td>
</tr>
<tr>
<td>AMOUNT</td>
<td>Order amount (not multiplied by 100)</td>
</tr>
<tr>
<td>BRAND</td>
<td>Card brand (our system derives this from the card number)</td>
</tr>
<tr>
<td>CARDNO</td>
<td>Masked card number</td>
</tr>
<tr>
<td>CN</td>
<td>Cardholder/customer name</td>
</tr>
<tr>
<td>CURRENCY</td>
<td>Order currency</td>
</tr>
<tr>
<td>ED</td>
<td>Expiry date</td>
</tr>
<tr>
<td>NCERROR</td>
<td>Error code</td>
</tr>
<tr>
<td>ORDERID</td>
<td>Your order reference</td>
</tr>
<tr>
<td>PAYID</td>
<td>Payment reference in our system</td>
</tr>
<tr>
<td>PM</td>
<td>Payment method</td>
</tr>
<tr>
<td>SHASIGN</td>
<td>SHA signature calculated by our system (if SHA-OUT configured)</td>
</tr>
<tr>
<td>STATUS</td>
<td>Transaction status (see Status overview)</td>
</tr>
<tr>
<td>TRXDATE</td>
<td>Transaction date</td>
</tr>
</tbody>
</table>

**Example (GET request)**

```
```

The list of feedback parameters can be longer if you have activated certain options in your account, such as the Fraud detection module. Please refer to the respective option documentation for more information on extra feedback parameters linked to the option.

#### 7.5.1 Dynamic feedback parameters

You may also choose which parameters are returned.

To do this, go to the "Transaction feedback" tab of your Technical information page, where you will see a list of "Available" and "Selected" fields. Only the "Selected" fields will be part of the feedback request.

To add or remove parameters from the feedback request, click on the parameter name and click the appropriate arrow to add/remove it to/from the list.

If you add/remove parameters from this list, do not forget to update your SHA-OUT signature accordingly. Parameters that are not selected here will NOT be contained in the SHA-OUT calculation.
7.5.2 Variable feedback parameters

You can send us two extra parameters in the hidden fields of the order form, in order to retrieve them as feedback parameter after the transaction. The following hidden fields are available:

- `<input type="hidden" name="COMPLUS" value=""/>
- `<input type="hidden" name="PARAMPLUS" value=""/>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLUS</td>
<td>Field for submitting a value you would like to be returned in the feedback request.</td>
</tr>
<tr>
<td>PARAMPLUS</td>
<td>Field for submitting some parameters and their values you would like to be returned in the feedback request. The field PARAMPLUS is not included in the feedback parameters as such; instead, the parameters/values you submit in this field will be parsed and the resulting parameters added to the http request.</td>
</tr>
</tbody>
</table>

Example

Extra hidden fields sent:

- `<input type="hidden" name="COMPLUS" value="123456789123456789123456789"/>
- `<input type="hidden" name="PARAMPLUS" value="SessionID=126548354&ShopperID=73541312"/>

resulting in a redirection with the feedback parameters:

https://www.yourwebsite.com/acceptpage.asp?...standard.parameters...]&COMPLUS=123456789123456789123456789&SessionID=126548354&ShopperID=73541312

7.6 Feedback reinitialization

In the event that a redirection/feedback request was not performed due to a blocking action by the customer on our secure payment pages (e.g. clicking the back button in the browser), we can reinitiate the post-payment request and/or redirection so your customer will be redirected to the page you want to display and your databases can be updated.

To enable this feature in your account, go to Configuration > Technical information > Transaction feedback > General, and tick the box "I would like PostFinance to re-launch the "end of transaction" (post-payment request/redirection) process if required."

It is possible, however, that you will receive multiple post-payment requests for the same Order ID, since the redirection/feedback request will be resubmitted if the customer returns to our secure payment pages using the back button after having been redirected to your website.

Please ensure you configure your Post URL script to handle these "exceptions". For example, you could configure your Post URL script to create a row in your database for each transaction status posted back, and/or generate an email to inform the merchant of an "exception" to the "expected" steps in the transaction process.

It is recommended that you do not overwrite the first transaction status message you receive with any subsequent messages you receive for the same Order ID - ideally you would store all responses for any order, and invoke a process whereby these can be investigated and dealt with appropriately.
If you do not enable this feature, when the customer clicks the back button to return to the secure payment pages, he will see a message indicating that the payment has already been processed.

7.7 Confirmation emails

7.7.1 Email to the merchant

Our system can send you a payment confirmation email for each transaction. You can configure this in the “E-mails to the merchant” section of the “Transaction e-mails” tab in your Technical information page.

In the same section, you can also choose to receive emails to be notified of transaction status changes.

7.7.2 Email to the customer

Our system can send an automatic email to your customer notifying him of the transaction registration. This is a standard email whose contents cannot be changed. The sender (“From”) address used when sending the email, is the address you entered in the “E-mail address(es) for transaction-related e-mails” field. If you entered more than one email address in this field, the first one in the row will be used.

You can activate this option in the “Transaction e-mails” tab, “E-mails to the customer” section of the Technical Information page.

You can also choose to send emails to the customer when the transaction is confirmed (data capture) and when a transaction is refunded, by ticking the corresponding boxes. As the sender (“From”) email address for these emails, you can configure the “Support E-mail address to include in transaction-related e-mails”. If you don't enter an email address here, we will use the first one entered in the “Support E-mail address to include in transaction-related e-mails” in the “E-mails to the merchant” section.

To be able to send confirmation emails to your customers, you must include the customer's email address in the hidden field:

<input type="hidden" name="EMAIL" value="">

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMAIL</td>
<td>Customer’s email address</td>
</tr>
</tbody>
</table>
8. Payment link via e-mail

You can send your customers a payment request by email, redirecting the customer to our secure payment page via a button or link in the email.

If the email is in HTML format you can use a form with hidden HTML fields to send us the necessary parameters in POST format.

If the email is in plain text format you can append the necessary parameters to the URL in GET format. (e.g. https://e-payment.postfinance.ch/ncol/test/orderstandard.asp/orderstandard_utf8.asp?PSPID=TESTSTD&OrderID=order123&amount=12500&currency=EUR&SHASIGN=8DDF4795640EB9FE9B367315C48E47338129A4F5& ...)

For more information, go to Link your website to the payment page.

For e-Commerce via email to work, you must bear in mind the following verification related points before the payment:

- You must leave the referrer/URL field in the URL field in the “Data and origin verification” tab, “ Checks for e-Commerce” section of the Technical information page in your account empty, in order to avoid unknown order/1/r errors.
- You must use an SHA signature as the data verification method for the order details. For further details about the SHA-IN, go to SHA-IN Signature.
9. Payment method selection options

9.1 Payment method selection on the merchant’s site

9.1.1 How to show a specific payment method

When a customer is redirected from your website/shop to our secure payment page, he will be presented with the payment methods that are activated in your PostFinance account.

However, if you want the selection of the payment methods to be done on your own website instead of on our payment page, you can send us the payment method name and/or brand in the hidden fields. In that case, we will only show this particular payment method on our payment page and the customer will be allowed to only pay with this payment method.

The additional hidden fields that you will send are the following:

<input type="hidden" name="PM" value="">
<input type="hidden" name="BRAND" value="">

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PM</td>
<td>Payment method or payment method group (e.g. credit card)</td>
</tr>
<tr>
<td>BRAND</td>
<td>Payment method brand (e.g. VISA)</td>
</tr>
</tbody>
</table>

Depending on the payment method, you will have to send both fields or only one of them. In many cases the PM and BRAND have the same value, in which case you can send only the PM or only the BRAND.

Examples

- Hidden fields in the event that you want your customer to pay with VISA:

<input type="hidden" name="PM" value="CreditCard ">
<input type="hidden" name="BRAND" value="VISA">

- Hidden fields in the event that you only want your customer to pay by credit card (other payment methods than credit cards won’t be displayed):

<input type="hidden" name="PM" value="CreditCard ">
<input type="hidden" name="BRAND" value="">

- Hidden fields in the event that you want your customer to pay with iDEAL:

<input type="hidden" name="PM" value="iDEAL">
<input type="hidden" name="BRAND" value="">

OR

<input type="hidden" name="PM" value="">
<input type="hidden" name="BRAND" value="iDEAL">

9.1.2 How to return from the payment page to the payment method selection screen
If the customer selects the payment method on your website, we will only present the selected payment method on the payment page to the customer.

If the payment with this payment method is unsuccessful and the customer would like to try using another payment method, he will not be presented with a list of your payment methods on our secure payment page, as the payment method selection took place on your website (and not on our secure payment page).

Therefore, to redirect the customer to a URL on your own website, where he can select another payment method, you can use the “BACKURL”.

With the BACKURL, when the customer clicks the “Back” button on our secure payment page, after the authorisation has been declined or after having cancelled from a third-party or bank website, we redirect him to the URL you have entered for the “BACKURL”.

**Note:** The “back” button described in this section is the back button in our secure payment pages, NOT the back button of the browser.

You can enter the “BACKURL” specified in the “Payment page” tab of your account’s “Technical information” page.

However if you prefer not to always use the same URL, you can also send us a specific “BACKURL” in the hidden fields. The “BACKURL” sent in the hidden fields will override the general “BACKURL” entered in your account.

You can send the “BACKURL” in the following hidden field:

```html
<input type="hidden" name="BACKURL" value=""/>
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKURL</td>
<td>URL of the web page to display to the customer when he clicks the “Back” button on our secure payment page.</td>
</tr>
</tbody>
</table>

If the customer selects the payment method on our secure payment page and not on your website, the “BACKURL” is not taken into account. Consequently, when the customer clicks the “Back” button on our secure payment page, he will simply be redirected to our secure payment method selection page.

### 9.2 Show a specific list of payment methods

If the customer is to select the payment method from a specific list of payment methods on our payment page, you can send us this list of payment methods in the hidden fields, so we will only show these specific payment methods on our payment page.

The hidden field is the following:

```html
<input type="hidden" name="PMLIST" value=""/>
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMLIST</td>
<td>List of selected payment methods and/or credit card brands. Separated by a “;” (semicolon).</td>
</tr>
</tbody>
</table>

**Example**

If you only want your customer to choose between VISA and iDEAL on our payment page (i.e. if you also have other payment methods that you don’t want to be displayed), the hidden field and its value will be:

```html
<input type="hidden" name="PMLIST" value="VISA;IDEAL"/>
```
9.3 Exclude specific payment methods

If you wish to not present a specific payment method to the customer, you can use a hidden field to do so. This is particularly useful for sub-brands, when you want to accept a brand (e.g. MasterCard) but not one of its sub-brands (e.g. Maestro).

The hidden field is the following:

```html
<input type="hidden" name="EXCLPMLIST" value="">
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXCLPMLIST</td>
<td>List of payment methods and/or credit card brands that should NOT be shown. Separated by a &quot;;&quot; (semicolon).</td>
</tr>
</tbody>
</table>

9.4 Layout of the payment methods

You can arrange the layout/list of the payment methods on our payment page using the following hidden field:

```html
<input type="hidden" name="PMLISTTYPE" value=""> 
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMLISTTYPE</td>
<td>The possible values are 0, 1 and 2:</td>
</tr>
<tr>
<td></td>
<td>• 0: Horizontally grouped logos with the group name on the left (default value)</td>
</tr>
<tr>
<td></td>
<td>• 1: Horizontally grouped logos with no group names</td>
</tr>
<tr>
<td></td>
<td>• 2: Vertical list of logos with specific payment method or brand name</td>
</tr>
</tbody>
</table>

9.5 Window for 3-D Secure

9.5.1 3-D Secure v1.0

If you have payment methods with 3-D Secure enabled, you can choose how you want the identification page to be displayed to the customer by sending us an extra parameter in the hidden fields.

The hidden field is the following:

```html
<input type="hidden" name="WIN3DS" value=""> 
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIN3DS</td>
<td>• &quot;MAINW&quot;: to display the identification page in the main window (default value);</td>
</tr>
<tr>
<td></td>
<td>• &quot;POPUP&quot;: to display the identification page in a POPUP window and return to the main window at the end.</td>
</tr>
</tbody>
</table>

Important

Please note that for some payment methods (e.g. Visa, MasterCard, JCB, etc.), the ‘POPUP’ value is not allowed and will be converted into ‘MAINW’ by the system. We recommend explicitly testing the behaviour of this field for every payment method.

9.5.2 3-D Secure v2.1 (Available in TEST)
In addition to the previously requested parameter (WIN3DS), it is **highly recommended** to include the following parameter. It contains the preconfigured sizes for width x height in pixels of the window displayed in the Cardholder browser window.

Note: If you don’t send this parameter, then the default value will be 05 = Full screen.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mpi.challengeWindowSize</td>
<td>• 01 = 250 x 400</td>
</tr>
<tr>
<td></td>
<td>• 02 = 390 x 400</td>
</tr>
<tr>
<td></td>
<td>• 03 = 500 x 600</td>
</tr>
<tr>
<td></td>
<td>• 04 = 600 x 400</td>
</tr>
<tr>
<td></td>
<td>• 05 = Full screen</td>
</tr>
</tbody>
</table>

In order to make the 3DS v2 approach to risk evaluation more effective, we recommend that you send in additional parameters as described in the list here. Providing these parameters can have a direct impact on your conversion rate as they can help authenticate the cardholder without being redirected. For more information refer to the DirectLink 3DS guide.

You can use the following test card to simulate a 3-D Secure registered card in our test environment:

### Frictionless Flow

<table>
<thead>
<tr>
<th>Brand</th>
<th>Card number</th>
<th>Expiry date</th>
</tr>
</thead>
<tbody>
<tr>
<td>VISA</td>
<td>4186455175836497</td>
<td>Any date in the future</td>
</tr>
<tr>
<td>Mastercard</td>
<td>5137009801943438</td>
<td>Any date in the future</td>
</tr>
<tr>
<td>American Express</td>
<td>375418081197346</td>
<td>Any date in the future</td>
</tr>
</tbody>
</table>

### Challenge Flow

<table>
<thead>
<tr>
<th>Brand</th>
<th>Card number</th>
<th>Expiry date</th>
</tr>
</thead>
<tbody>
<tr>
<td>VISA</td>
<td>4874970686672022</td>
<td>Any date in the future</td>
</tr>
<tr>
<td>Mastercard</td>
<td>5130257474533310</td>
<td>Any date in the future</td>
</tr>
<tr>
<td>American Express</td>
<td>379764422997381</td>
<td>Any date in the future</td>
</tr>
</tbody>
</table>

Note: More test cards numbers can be downloaded here.

### 9.6 Split credit/debit cards

The functionality to split VISA and MasterCard into a debit and a credit payment method allows you to offer them to your customers as two different payment methods (e.g. VISA Debit and VISA Credit), or you can decide only to accept one of both split brands.

To use the split of credit and debit cards via e-Commerce, you need to include the CREDITDEBIT parameter in the hidden fields that you send to the payment page (and therefore also include in the SHA-IN calculation).
Field | Format
--- | ---
CREDITDEBIT | “C”: credit card
| “D”: debit card

Related error: When the buyer selects the debit card method but next enters a credit card number, an error code will be returned: ‘Wrong brand/Payment method was chosen’.

If the payment is successfully processed with the CREDITDEBIT parameter, the same parameter will also be returned in the post-sale feedback. However, whereas the submitted values are C or D, the return values are “CREDIT” or “DEBIT”.

You will also find these return values in transaction overview via “View transactions” and “Financial history”, and in reports you may download afterwards.

Configuration in your account

The split functionality can also be activated and configured per payment method, in your PostFinance account. Go to Split Credit/Debit Cards for more information.
10. Optional fields

10.1 Operation

Important

The ability to work in two stages (authorisation + data capture) depends on the payment methods you wish to use. (See the “Payment Methods Processing/Procedure overview” in the Support section of your account).

If you prefer not to use the same operation code as selected in the "Global transaction parameters" tab, in the "Default operation code" section of the “Technical Information” page in your account for a given transaction, you can send us a specific operation code for this transaction.

The operation code you send us in the hidden fields will override the default operation code selected in the "Default operation code" section of the "Global transaction parameters" tab, on the “Technical information” page in your account. You can send the operation code with the following hidden field:

```
<input type="hidden" name="OPERATION" value="">
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPERATION</td>
<td>Operation code for the transaction. Possible values for new orders:</td>
</tr>
<tr>
<td></td>
<td>• RES: request for authorization</td>
</tr>
<tr>
<td></td>
<td>• SAL: request for sale (payment)</td>
</tr>
<tr>
<td></td>
<td>Optional</td>
</tr>
</tbody>
</table>

In order for this parameter to be taken into account by our system, it needs to be included in the SHA-IN signature calculation for the transaction.

10.2 User field

If you have multiple users in your account and you want to register transactions associated with a specific user (e.g. for call centre agents logging transactions via e-Commerce), you can send the USERID in the following hidden field:

```
<input type="hidden" name="USERID" value="">
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERID</td>
<td>The username specified in the account’s user management page</td>
</tr>
</tbody>
</table>
This field is just an informative field to add a USERID to a specific transaction. We do not perform any check at our end to establish e.g. if there have been password errors for this user. The only check we perform is to verify that the USERID is valid. If the USERID does not exist, we will replace it by the default USERID of the account (PSPID).