Basic e-Commerce

Technical integration guide for e-Commerce v.3.3

Table of Contents

1 Introduction

This document explains the basic integration procedure for the e-Commerce module.

Basic e-Commerce complements the Back-Office User Guide. Please refer to the Back-Office User Guide for the configuration and functionality of the administration site and the description of other products.

For more detailed integration information, please refer to the Advanced e-Commerce Integration Guide.

2 Test Environment

We recommend that you perform your integration in our test environment before going live in the production environment. Our test environment works almost identically to our production environment, except for the fact that we don't send the transactions to the card acquirer or invoice you.

Our test environment allows you to make test payments, change your account configuration and fine-tune the integration of our payment system on your website.

2.1 Creating a test account

- To open a free test account, visit our website at http://www.ogone.com.
- Click the link "Create your free test account" at the top of the page.
- Complete the form (with correct information, as we shall send the password to the email address you enter!) and click the "Register" button.
- Wait for the confirmation email and the email containing your password (this might take a little while, as we check the details you enter).

2.2 Accessing your test account

When you receive the password for your test account by email, you can access your account as follows:

- Visit our website at http://www.ogone.com.
- Click the "Test account" under 'Merchant Login' at the top of the page. link.
- Enter the PSPID you chose when registering your account and the (case-sensitive!) password you received by email. Click on "Submit".

When you log in for the first time using a password you received by email, you will be requested to change the password immediately to a value of your choice.

2.3 Configuring your test account

When you first log into your account, you will see a list of steps to complete on the homepage. These steps concern the administrative, payment method and technical details of your test account. The configuration of the administrative details is self-explanatory. The configuration of the payment methods and the technical details is explained below.

You can start the configuration by clicking the first link. In one of the steps, you have to enter your billing details. In the test environment, you will not receive any bills, but you will nevertheless be asked to enter this information. You can choose "Credit card" as the charging method and enter the VISA test card number 4111111111111111, with an expiry date some time the future, or you can select the "NOT BILLED" option.

Once all the steps have been completed, you can ask to activate your test account.

If your account has been activated and you would like to change some details, you can still call up the various configuration pages via your menu. This is especially useful with regard to the "Technical information" page, as you might want to change some details while testing your integration.

2.3.1 Configuring the payment methods

To select a payment method you want to use in your account, simply click the "Add" button next to the payment method in the available payment method list and fill out the card affiliation request. In the test environment, you can complete the form with fake details. However, in the production environment, you have to fill in the correct affiliation details for your acquirer, which can be found in the contract signed with your acquirer.

The payment method will be added to the "Selected payment method" list.

You can access the payment methods configuration page via the “Payment methods” link in the Configuration menu.

2.3.2 Configuring the technical information

The following chapters will help you configure the Technical information page in your account. At the beginning of each chapter you will see a reference to the related items on the Technical information page or on your website, depending on where you need to take action.

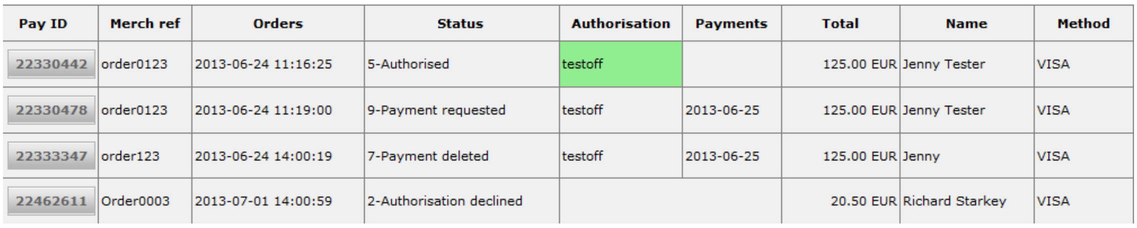
You can access the technical parameters via the “Technical information” link in your menu.

2.4 Test transactions and their results

Once your account is fully configured and active, you can start performing test payments.

You can perform test payments from your website, or from a test page on our server, available in the “Test info” tab on your “Technical information” page, which simulates the last page of your shopping basket. You can use this test page if you would like to start performing test payments, but haven’t fully finished the integration into your website.

You can perform a test payment following the sale process. After you have performed a transaction, you can view the details in the back office of your account. When you have logged in, click the "View transactions" link in your menu, enter your selection criteria (the first time, enable all the status check boxes and leave the other fields with their default values) and view the result list. Check the Back-Office User Guide for further information on the use of the back-office in your account.



Pay ID	Merch ref	Orders	Status	Authorisation	Payments	Total	Name	Method
22330442	order0123	2013-06-24 11:16:25	5-Authorised	testoff		125.00 EUR	Jenny Tester	VISA
22330478	order0123	2013-06-24 11:19:00	9-Payment requested	testoff	2013-06-25	125.00 EUR	Jenny Tester	VISA
22333347	order123	2013-06-24 14:00:19	7-Payment deleted	testoff	2013-06-25	125.00 EUR	Jenny	VISA
22462611	Order0003	2013-07-01 14:00:59	2-Authorisation declined			20.50 EUR	Richard Starkey	VISA

The most frequent transaction statuses are:

0 - Invalid or incomplete

1 - Cancelled by customer

2 - Authorisation declined

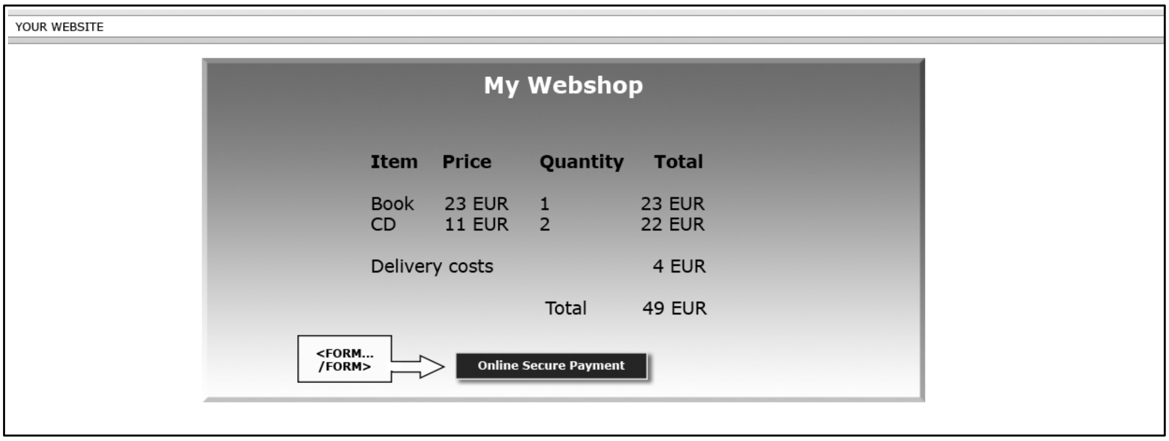
5 - Authorised

9 - Payment requested

More information about statuses and error codes can be found in your Ogone account. Just log in and go to: Support > Integration & user manuals > User guides > List of the payment statuses and error codes.

3 Sale Process

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



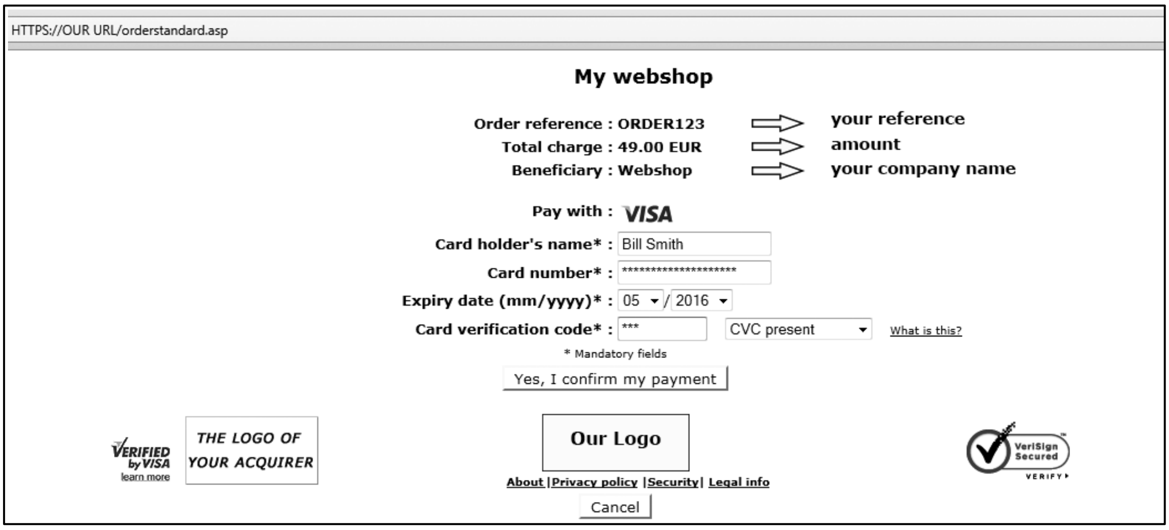
YOUR WEBSITE

My Webshop

Item	Price	Quantity	Total
Book	23 EUR	1	23 EUR
CD	11 EUR	2	22 EUR
Delivery costs			4 EUR
		Total	49 EUR

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 here: Link between the merchant's website and our payment page.



HTTPS://OUR URL/orderstandard.asp

My webshop

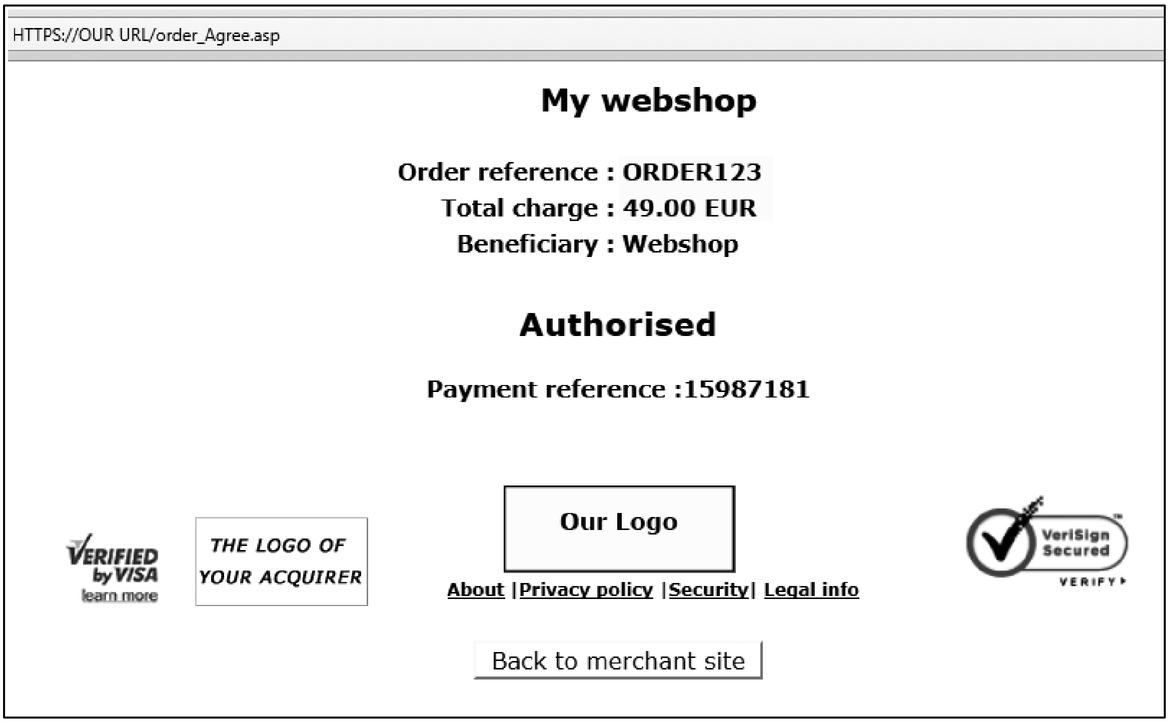
Order reference : ORDER123 → your reference
Total charge : 49.00 EUR → amount
Beneficiary : Webshop → your company name

Pay with : VISA
Card holder's name* : Bill Smith
Card number* : ********************
Expiry date (mm/yyyy)* : 05 / 2016
Card verification code* : *** CVC present What is this?
* Mandatory fields

Yes, I confirm my payment
VERIFIED by VISA learn more
THE LOGO OF YOUR ACQUIRER
Our Logo
About | Privacy policy | Security | Legal info
Cancel
VeriSign Secured VERIFY

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.



HTTPS://OUR URL/order_Agree.asp

My webshop

Order reference : ORDER123
Total charge : 49.00 EUR
Beneficiary : Webshop

Authorised

Payment reference :15987181

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 Transaction feedback to the customer.

4 General payment parameters

Important

This chapter only applies for payment methods such as credit cards, which allow you to reserve the customer's money without charging the customer straight away.

The ability to work in two steps (authorisation + data capture) and the ability to work online or offline depends on the payment methods you wish to use (see the online Payment Methods Processing/Procedure overview).

Where to configure? Technical Information – Global transaction parameters tab

4.1 Default operation code and default data capture (payment) procedure

For some payment methods (mainly credit cards), transactions are performed in two steps: the authorisation and the data capture (payment request).

During the authorisation step, the transaction amount is either reserved on the customer's card/ account, or the request data is matched against one or more fraud detection blacklists.

In the data capture (payment request) step, your acquirer is requested to take the reserved amount from the customer's card/account and transfer it to your bank account.

Based on these two steps you can choose between two default operation codes:

- Authorisation: our system will only ask for an authorisation, in order to have the authorisation and data capture (payment request) steps performed separately, at different times (the money remains in the customer's account until the relevant data has been captured (payment request)).

- Sale: our system automatically requests the payment (transfer of the amount) immediately after successful authorisation. This procedure is often used for goods/services delivered online.

If you have "Authorisation" as the default operation code for your account or you included the "Authorisation" operation code in the transaction details, the relevant transaction data will have to be captured in order to request the payment.

Three possible data capture (payment request) procedures are available:

- Data capture by the merchant (manual or automatic): to request the transfer of the reserved amount to your bank account, you must call up your administration module and request the data capture (payment) for the specific transaction.

  You can also automate the data process by sending us the data captures via batch or via a server-to-server request.

  This procedure is often used if the merchant has to check his stocks before dispatching the ordered goods.

- Automatic data capture by our system at the end of the day: our system requests the payment (data capture) automatically as from midnight, GMT+1 time.

- Automatic data capture by our system after x days: our system requests the payment (data capture) automatically after x days (if you have not cancelled the authorisation).

  The minimum number of days you can enter is "2" since "1" would lead the payment to be requested automatically as from midnight, i.e. an "Automatic data capture by our system at the end of the day".

This procedure is often used for goods/services delivered within a specific time.

4.2 Processing for individual transactions

There are three ways of processing for individual transactions:

- Always online (Immediate): the transaction request is sent to the acquirer immediately while the customer is connected (appropriate for goods/services delivered online).
- Online but switch to offline in intervals when the online acquiring system is unavailable: if you want online processing but do not want to miss out on transactions if the online acquirer clearing system is temporarily unavailable, you can authorise offline processing in these specific circumstances.

  We will store the transactions arriving from your website during the unavailability of your acquirer and will process them offline as soon as the acquirer clearing system is back up again. (N.B. This is not suitable for services that are triggered online immediately after the transaction!)
- Always offline (Scheduled): we register the transaction and process it afterwards (max. 4 hours). This method is slightly faster for the customer, as we do not send the request to the acquirer immediately (can be used for goods/services that do not need to be delivered online) . However, the customer will not immediately see the transaction/order result. Offline processing is not supported by all payment methods.

5 Link between the merchant's website and our payment page

Where to configure? Your website (shopping basket)

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:

```
<form method="post" action="https://secure.ogone.com/ncol/test/orderstandard.asp" id=form1 name=form1>
<!-- general 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="">
<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="">
<!-- post payment redirection: see Transaction feedback to the customer -->
<input type="hidden" name="ACCEPTURL" value="">
<input type="hidden" name="DECLINEURL" value="">
<input type="hidden" name="EXCEPTIONURL" value="">
<input type="hidden" name="CANCELURL" value="">
```

```
<input type="submit" value="" id=submit2 name=submit2>

</form>
```

Although the mandatory parameters are the PSPID, ORDERID, AMOUNT, CURRENCY and LANGUAGE value, we nevertheless strongly recommend you to also send us the customer name (CN), customer's email (EMAIL), address (OWNERADDRESS), town (OWNERTOWN), postcode (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 (the other fields are described in the following chapters):

Field	Usage
PSPID	Your affiliation name in our system
ORDERID	Your order number (merchant reference). The system checks that a payment has not been requested twice for the same order. The ORDERID has to be assigned dynamically.
AMOUNT	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.
CURRENCY	Currency of the order in ISO alpha code, e.g. EUR, USD, GBP, etc.
LANGUAGE	Language of the customer. For instance: en_US, nl_NL, fr_FR, etc.
CN	Customer name. Will be pre-initialised (but still editable) in the Customer Name field of the credit card details.
EMAIL	Customer's email address
OWNERADDRESS	Customer's street name and number
OWNERZIP	Customer's postcode
OWNERTOWN	Customer's town/city name
OWNERCTY	Customer's country
OWNERTELNO	Customer's telephone number

More information about these fields can be found in your Ogone account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

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://secure.ogone.com/ncol/test/orderstandard.asp
In the PRODUCTION environment the URL for the action will be https://secure.ogone.com/ncol/prod/orderstandard.asp

Important

When you switch to your PRODUCTION account, you have to replace "test" with "prod". 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.

6 Security: Check prior to Payment

Where to configure? Technical Information – Data and origin verification tab – Checks for e-Commerce section

6.1 Referrer

Our system checks the origin of the payment request, i.e. the URL (webpage) from which the order originated. This URL is called the referrer.

You must enter the URL of your webpage, containing the order form with the hidden fields, in the URL field in your account: Technical information page, "Data and origin" tab, in the "Checks for e-Commerce" section.

You can enter different URLs, separated by a semicolon (;). The URL(s) must always start with http:// or https://.

If the payment page is called from a URL that is not put in the referrer field, the *"unknown order/1/r"* error will occur.

6.2 SHA-IN signature

We propose SHA-1, SHA-256 and SHA-512 as data check methods. For each order, your server generates a unique character string (called a digest), hashed with the SHA algorithm of your choice.

6.2.1 Creating the string

This string 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 merchant's Technical information page, 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 be hashed.
- All parameter names should be in UPPERCASE (to avoid any case confusion).
- All parameters need to be arranged alphabetically
- 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.
- Parameters that do not have a value should NOT be included in the string to hash
- When you choose to transfer your test account to production via the link in the account menu, a random SHA-IN passphrase will be automatically configured in your production account.
- For extra safety, we request that you to use different SHA passphrases in test and production. 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).

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 recompose 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.

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

Parameters (in alphabetical order)

AMOUNT: 15.00 -> 1500
CURRENCY: EUR
LANGUAGE: en_US
ORDERID: 1234
PSPID: MyPSPID

SHA-IN passphrase (in Technical information)
Mysecretsig1875!?

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 additional string (password/passphrase) entered in the SHA-IN passphrase field in the "Data and origin verification" tab, in the “Checks for e-Commerce” section of the Technical information page, you will receive the error message *“unknown order/1/s".*

If nothing is sent in the "SHASIGN" field in the hidden HTML fields, even though an additional string (password/passphrase) has been entered in the SHA-IN passphrase field in the "Data and origin verification" tab, “Checks for e-Commerce” section of 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:

Field	Usage
SHASIGN	Unique character string for order data validation. A string hashed with the SHA-1 algorithm will always be 40 characters long.

More information about these fields can be found in your Ogone account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

6.2.2 SHA-1 module

To be able to hash a string and send it to us, you must first install an Encryption module on your server.

SHA-1, SHA-256 and SHA-512 modules can be found on the internet, so you will not have any problem in finding a suitable one for your server. To help you find a module for your environment, we have compiled the following list of sites:

General info on SHA at W3.org:

http://www.w3.org/PICS/DSig/SHA1_1_0.html

.NET / SHA1:

http://msdn2.microsoft.com/en-us/library/system.security.cryptography.sha1managed.aspx

PHP / SHA1:

http://www.php.net/manual/en/ref.mhash.php

7 Look and feel of the payment page

Where to configure? Your website (shopping basket)

When our e-Commerce system requests the customer for his credit card details, the customer is on our secure server. To maintain your website's look during the payment process, you can customise our static template.

The static template page has a generic format at our end, but you can change the look of some elements on the payment page or include your logo by simply adding some hidden fields in the form you send us.

The following table gives the hidden fields used to transmit the look and feel parameters to our system:

Field	Usage	Default value
TITLE	Title and header of the page	_
BGCOLOR	Background colour	white
TXTCOLOR	Text colour	black
TBLBGCOLOR	Table background colour	white
TBLTXTCOLOR	Table text colour	black
BUTTONBGCOLOR	Button background colour	_
BUTTONTXTCOLOR	Button text colour	black
FONTTYPE	Font family	verdana
LOGO	URL/filename of the logo you want to display at the top of the payment page next to the title. The URL must be absolute (contain the full path), it cannot be relative. If you don't have a secure environment to store your image, you can send us your image (JPG, PNG or GIF file) in an email (with your PSPID in the subject) to support@ogone.com (only for active production accounts). Please make sure the "Logo hosting" option is active in "Account" > "Your options" before sending us your logo). If the logo is stored on our servers, the URL will be: https://secure.ogone.com/ncol/images/*[PSPID]/[image]*	_

More information about these fields can be found in your Ogone account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

The colours can be specified by their hexadecimal code (#FFFFFF) or their name (white). We recommend you check first how the colours you want to use appear in different browsers.

It is also possible to use a specific template or a dynamic template. However, this requires advanced integration. You can find more information on this in the Advanced e-Commerce Integration Guide.

8 Transaction feedback to the customer

Where to configure? Your website (shopping basket), Technical information – Transaction emails tab – Emails to the customer

8.1 On screen

If you don't specify anything, our system shows the customer a standard message: "Your payment is accepted" or "The transaction has been denied". This message is inserted into the template (payment) page, which also contains a link to your homepage.

However, you can also redirect the customer to an HTML page on your website, depending on the payment result. In the hidden fields of your ordering form, you can send four URLs (ACCEPTURL, EXCEPTIONURL, CANCELURL and DECLINEURL) where our system redirects the customer to at the end of the payment process:

Following are the hidden fields used to transmit the URLs:

Field	Usage
ACCEPTURL	URL of the web page to show the customer when the payment is authorised (status 5), accepted (status 9) or waiting to be accepted (pending status 51 or 91).
DECLINEURL	URL of the web page to show the customer when the acquirer refuses the authorisation (status 2) up to the maximum authorised number of attempts.
EXCEPTIONURL	URL of the web page to show the customer when the payment result is uncertain (status 52 or 92). If this field is empty, the customer will be referred to the ACCEPTURL instead.
CANCELURL	URL of the web page to show the customer when he cancels the payment (status 1). If this field is empty, the customer will be redirected to the DECLINEURL instead.

More information about these fields can be found in your Ogone account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

You can also configure these URLs on the Technical information page of your account: "Transaction feedback" tab, in the "HTTP redirection in the browser" section.

8.2 By email

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 "Email address(es) for transaction-related emails" 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 emails" tab, "Emails 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 Email address to include in transaction-related emails". If you don't enter an email adress here, we will use the first one entered in the "Support Email address to include in transaction-related emails" in the "Emails 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="">
```

Field	Description
EMAIL	Customer’s email address

More information about these fields can be found in your Ogone account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

8.3 Other (Advanced)

It is also possible to show the customer a highly personalised response in the browser, or just an additional text on our standard response page. However, this requires advanced integration. You can find more information on these options in the Advanced e-Commerce Integration Guide.

9 Transaction feedback to the merchant

Where to configure? Your website (database), Technical Information > Transaction emails tab > Emails to the merchant section, Technical Information > Transaction feedback tab > HTTP redirection in the browser section.

9.1 Back office

You can always view the transaction results in the back office of your account. When you have logged in, click the “Financial history” or "View transactions" link in your menu, enter your selection criteria and view the result list. Please refer to the Back-Office User Guide for further information about using the back office in your account.

9.2 By email

You can receive a payment confirmation email from our system for each transaction (option to configure in the Technical information > "Transaction emails" tab > "Emails to the merchant" section).

9.3 Request on your page

When a payment is captured, we can send the below listed parameters in a request on your ACCEPTURL, EXCEPTIONURL, CANCELURL or DECLINEURL to enable you to perform a database update.

You can activate this option in the Technical information page > "Transaction feedback" tab > "HTTP redirection in the browser" section: “I would like to receive transaction feedback parameters on the redirection URLs”.

Parameter	Value
orderID	Your order reference
amount	Order amount (NOT multiplied by 100) Decimals only returned when relevant - not for whole amounts, e.g. 15, 15.1, 15.12
currency	Currency of the order
PM	Payment method
ACCEPTANCE	Acceptance code returned by acquirer
STATUS	Transaction status
CARDNO	Masked card number
PAYID	Payment reference in our system
NCERROR	Error code
BRAND	Card brand (our system derives it from the card number) or similar information for other payment methods.
SHASIGN	SHA signature composed by our system, if SHA-OUT is configured by you.

More information about these fields can be found in your Ogone account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

Important

You have to use an SHA signature to verify the request contents when you use this option, to prevent customers from tampering with details in the URL field to cause an incorrect database update.

If you do not configure an SHA-OUT signature we cannot send any parameters to your ACCEPTURL, EXCEPTIONURL, CANCELURL or DECLINEURL.

This string for the SHA is constructed by concatenating the fields and their values sent with the order (in the format "parameter=value", followed by a passphrase). The passphrase is defined in the merchant's Technical information page, under the “Feedback” tab, in the “All transaction submission modes” section. For the full list of parameters to include in the SHA Digest, please refer to the List of parameters to be included in SHA calculations in this guide.

Please note that the parameter names are case sensitive for the SHA calculation

In the same way we re-create the Digest to validate the input of the transaction with the SHA-IN, you must reconstruct the hash, this time using your SHA-OUT passphrase and the parameters, exactly as received from our system.

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

Please also make sure to take the following points into consideration:

- All sent parameters (that appear in the list in List of parameters to be included in SHA calculations (SHA-OUT)), will be included in the string to hash.
- All parameters must be sorted following the order in the List of parameters to be included in SHA calculations (SHA-OUT)
- 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 account 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).

Example of a SHA-1-OUT calculation with only basic parameters

Parameters (in alphabetical order):
ACCEPTANCE: 1234
amount: 15
BRAND: VISA
CARDNO: XXXXXXXXXXXX1111
currency: EUR
NCERROR: 0
orderID: 12
PAYID: 32100123
PM: CreditCard
STATUS: 9

SHA passphrase (in Technical information):
Mysecretsig1875!?

String to hash:
ACCEPTANCE=1234Mysecretsig1875!?AMOUNT=15Mysecretsig1875!?
BRAND=VISAMysecretsig1875!?CARDNO=XXXXXXXXXXXX1111Mysecretsig1875!?
CURRENCY=EURMysecretsig1875!?NCERROR=0Mysecretsig1875!?
ORDERID=12Mysecretsig1875!?PAYID=32100123Mysecretsig1875!?
PM=CreditCardMysecretsig1875!?STATUS=9Mysecretsig1875!?

Resulting Digest (SHA-1):
209113288F93A9AB8E474EA78D899AFDBB874355

Please refer to SHA-1 module for further general information about the SHA-1 module.

Character encoding for PostFinance payment methods

If you use UTF-8 character encoding for the integration of PostFinance Card and/or PostFinance E-finance, the transaction feedback will be returned ISO-8859-1 encoded.

9.4 Other (Advanced)

It is also possible to receive a request with transaction parameters from our end on a specific page at your end, which is not visible to the customer. However, this requires an advanced integration. You can find more information on this and other options in the Advanced e-Commerce Integration Guide.

10 Appendix: List of parameters to be included in SHA calculations

10.1 SHA-IN

ACCEPTANCE

ACCEPTURL

ADDMATCH

ADDRMATCH

AIACTIONNUMBER

AIAGIATA

AIAIRNAME

AIAIRTAX

AIBOOKIND*XX*

AICARRIER*XX*

AICHDET

AICLASS*XX*

AICONJTI

AIDEPTCODE

AIDESTCITY*XX*

AIDESTCITYL*XX*

AIEXTRAPASNAME*XX*

AIEYCD

AIFLDATE*XX*

AIFLNUM*XX*

AIGLNUM

AIINVOICE

AIIRST

AIORCITY*XX*

AIORCITYL*XX*

AIPASNAME

AIPROJNUM

AISTOPOV*XX*

AITIDATE

AITINUM

AITINUML*XX*

AITYPCH

AIVATAMNT

AIVATAPPL

ALIAS

ALIASOPERATION

ALIASPERSISTEDAFTERUSE

ALIASUSAGE

ALLOWCORRECTION

AMOUNT

AMOUNT*XX*

AMOUNTHTVA
AMOUNTTVA
ARP_TRN
BACKURL
BATCHID
BGCOLOR
BLVERNUM
BIC
BIN
BRAND
BRANDVISUAL
BUTTONBGCOLOR
BUTTONTXTCOLOR
CANCELURL
CARDNO
CATALOGURL
CAVV_3D
CAVVALGORITHM_3D
CERTID
CHECK_AAV
CIVILITY
CN
COM
COMPLUS
CONVCCY
COSTCENTER
COSTCODE
CREDITCODE
CREDITDEBIT
CUID
CURRENCY
CVC
CVCFLAG
DATA
DATATYPE
DATEIN
DATEOUT
DBXML
DCC_COMMPERC
DCC_CONVAMOUNT
DCC_CONVCCY
DCC_EXCHRATE
DCC_EXCHRATETS
DCC_INDICATOR
DCC_MARGINPERC
DCC_REF
DCC_SOURCE
DCC_VALID

DECLINEURL
DELIVERYDATE
DEVICE
DISCOUNTRATE
DISPLAYMODE
ECI
ECI_3D
ECOM_BILLTO_COMPANY
ECOM_BILLTO_POSTAL_CITY
ECOM_BILLTO_POSTAL_COUNTRYCODE
ECOM_BILLTO_POSTAL_COUNTY
ECOM_BILLTO_POSTAL_NAME_FIRST
ECOM_BILLTO_POSTAL_NAME_LAST
ECOM_BILLTO_POSTAL_NAME_PREFIX
ECOM_BILLTO_POSTAL_POSTALCODE
ECOM_BILLTO_POSTAL_STREET_LINE1
ECOM_BILLTO_POSTAL_STREET_LINE2
ECOM_BILLTO_POSTAL_STREET_LINE3
ECOM_BILLTO_POSTAL_STREET_NUMBER
ECOM_BILLTO_TELECOM_MOBILE_NUMBER
ECOM_BILLTO_TELECOM_PHONE_NUMBER
ECOM_CONSUMERID
ECOM_CONSUMER_GENDER
ECOM_CONSUMEROGID
ECOM_CONSUMERORDERID
ECOM_CONSUMERUSERALIAS
ECOM_CONSUMERUSERPWD
ECOM_CONSUMERUSERID
ECOM_ESTIMATEDDELIVERYDATE
ECOM_ESTIMATEDELIVERYDATE
ECOM_PAYMENT_CARD_EXPDATE_MONTH
ECOM_PAYMENT_CARD_EXPDATE_YEAR
ECOM_PAYMENT_CARD_NAME
ECOM_PAYMENT_CARD_VERIFICATION
ECOM_SHIPMETHOD
ECOM_SHIPMETHODDETAILS
ECOM_SHIPMETHODSPEED
ECOM_SHIPMETHODTYPE
ECOM_SHIPTO_COMPANY
ECOM_SHIPTO_DOB
ECOM_SHIPTO_ONLINE_EMAIL
ECOM_SHIPTO_POSTAL_CITY
ECOM_SHIPTO_POSTAL_COUNTRYCODE
ECOM_SHIPTO_POSTAL_COUNTY
ECOM_SHIPTO_POSTAL_NAME_FIRST
ECOM_SHIPTO_POSTAL_NAME_LAST
ECOM_SHIPTO_POSTAL_NAME_PREFIX
ECOM_SHIPTO_POSTAL_POSTALCODE

ECOM_SHIPTO_POSTAL_STATE
ECOM_SHIPTO_POSTAL_STREET_LINE1
ECOM_SHIPTO_POSTAL_STREET_LINE2
ECOM_SHIPTO_POSTAL_STREET_NUMBER
ECOM_SHIPTO_TELECOM_FAX_NUMBER
ECOM_SHIPTO_TELECOM_MOBILE_NUMBER
ECOM_SHIPTO_TELECOM_PHONE_NUMBER
ECOM_SHIPTO_TVA
ED
EMAIL
EXCEPTIONURL
EXCLPMLIST
EXECUTIONDATE*XX*
FACEXCL*XX*
FACTOTAL*XX*
FIRSTCALL
FLAG3D
FONTTYPE
FORCECODE1
FORCECODE2
FORCECODEHASH
FORCEPROCESS
FORCETP
FP_ACTIV
GENERIC_BL
GIROPAY_ACCOUNT_NUMBER
GIROPAY_BLZ
GIROPAY_OWNER_NAME
GLOBORDERID
GUID
HDFONTTYPE
HDTBLBGCOLOR
HDTBLTXTCOLOR
HEIGHTFRAME
HOMEURL
HTTP_ACCEPT
HTTP_USER_AGENT
INCLUDE_BIN
INCLUDE_COUNTRIES
INITIAL_REC_TRN
INVDATE
INVDISCOUNT
INVLEVEL
INVORDERID
ISSUERID
IST_MOBILE
ITEM_COUNT
ITEMATTRIBUTES*XX*

ITEMCATEGORY*XX*

ITEMCOMMENTS*XX*

ITEMDESC*XX*

ITEMDISCOUNT*XX*

ITEMFDMPRODUCTCATEG*XX*

ITEMID*XX*

ITEMNAME*XX*

ITEMPRICE*XX*

ITEMQUANT*XX*

ITEMQUANTORIG*XX*

ITEMUNITOFMEASURE*XX*

ITEMVAT*XX*

ITEMVATCODE*XX*

ITEMWEIGHT*XX*

LANGUAGE

LEVEL1AUTHCPC

LIDEXCL*XX*

LIMITCLIENTSCRIPTUSAGE

LINE_REF

LINE_REF1

LINE_REF2

LINE_REF3

LINE_REF4

LINE_REF5

LINE_REF6

LIST_BIN

LIST_COUNTRIES

LOGO

MANDATEID

MAXITEMQUANT*XX*

MERCHANTID

MODE

MTIME

MVER

NETAMOUNT

OPERATION

ORDERID

ORDERSHIPCOST

ORDERSHIPMETH

ORDERSHIPTAX

ORDERSHIPTAXCODE

ORIG

OR_INVORDERID

OR_ORDERID

OWNERADDRESS

OWNERADDRESS2

OWNERCTY

OWNERTELNO

OWNERTELNO2
OWNERTOWN
OWNERZIP
PAIDAMOUNT
PARAMPLUS
PARAMVAR
PAYID
PAYMENTOCCURRENCE
PAYMETHOD
PM
PMLIST
PMLISTPMLISTTYPE
PMLISTTYPE
PMLISTTYPEPMLIST
PMTYPE
POPUP
POST
PSPID
PSWD
RECIPIENTACCOUNTNUMBER
RECIPIENTDOB
RECIPIENTLASTNAME
RECIPIENTZIP
REF
REFER
REFID
REFKIND
REF_CUSTOMERID
REF_CUSTOMERREF
REGISTRED
REMOTE_ADDR
REQGENFIELDS
RNPOFFERT
RTIMEOUT
RTIMEOUTREQUESTEDTIMEOUT
SCORINGCLIENT
SEQUENCETYPE
SETT_BATCH
SID
SIGNDATE
STATUS_3D
SUBSCRIPTION_ID
SUB_AM
SUB_AMOUNT
SUB_COM
SUB_COMMENT
SUB_CUR
SUB_ENDDATE

SUB_ORDERID
SUB_PERIOD_MOMENT
SUB_PERIOD_MOMENT_M
SUB_PERIOD_MOMENT_WW
SUB_PERIOD_NUMBER
SUB_PERIOD_NUMBER_D
SUB_PERIOD_NUMBER_M
SUB_PERIOD_NUMBER_WW
SUB_PERIOD_UNIT
SUB_STARTDATE
SUB_STATUS
TAAL
TAXINCLUDED*XX*
TBLBGCOLOR
TBLTXTCOLOR
TID
TITLE
TOTALAMOUNT
TP
TRACK2
TXTBADDR2
TXTCOLOR
TXTOKEN
TXTOKENTXTOKENPAYPAL
TXSHIPPING
TXSHIPPINGLOCATIONPROFILE
TXURL
TXVERIFIER
TYPE_COUNTRY
UCAF_AUTHENTICATION_DATA
UCAF_PAYMENT_CARD_CVC2
UCAF_PAYMENT_CARD_EXPDATE_MONTH
UCAF_PAYMENT_CARD_EXPDATE_YEAR
UCAF_PAYMENT_CARD_NUMBER
USERID
USERTYPE
VERSION
WBTU_MSISDN
WBTU_ORDERID
WEIGHTUNIT
WIN3DS
WITHROOT

10.2 SHA-OUT

AAVADDRESS
AAVCHECK
AAVMAIL
AAVNAME

AAVPHONE

AAVZIP

ACCEPTANCE

ALIAS

AMOUNT

BIC

BIN

BRAND

CARDNO

CCCTY

CN

COLLECTOR_BIC

COLLECTOR_IBAN

COMPLUS

CREATION_STATUS

CREDITDEBIT

CURRENCY

CVCCHECK

DCC_COMMPERCENTAGE

DCC_CONVAMOUNT

DCC_CONVCCY

DCC_EXCHRATE

DCC_EXCHRATESOURCE

DCC_EXCHRATETS

DCC_INDICATOR

DCC_MARGINPERCENTAGE

DCC_VALIDHOURS

DEVICEID

DIGESTCARDNO

ECI

ED

EMAIL

ENCCARDNO

FXAMOUNT

FXCURRENCY

IP

IPCTY

MANDATEID

MOBILEMODE

NBREMAILUSAGE

NBRIPUSAGE

NBRIPUSAGE_ALLTX

NBRUSAGE

NCERROR

ORDERID

PAYID

PAYMENT_REFERENCE

PM

SCO_CATEGORY
SCORING
SEQUENCETYPE
SIGNDATE
STATUS
SUBBRAND
SUBSCRIPTION_ID
TRXDATE
VC