Basic e-Commerce

Technical integration guide for e-Commerce v.2.3.0

Table of Contents

1 Introduction

This document explains the basic integration procedure of 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 bill 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 since we'll send the password to the e-mail address you enter!) and click the "Register" button.
- Wait for the confirmation e-mail and the e-mail containing your password (this might take a little while since we check the details you enter).

2.2 Accessing your test account

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

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

When you log in for the first time using a password you received by e-mail, you'll be requested to change the password immediately to a value you choose yourself.

2.3 Configure your test account

When you first log into your account, you'll 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 pretty straightforward. 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 be asked to enter this information anyhow. 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 for your test account to be activated.

If your account has been activated and you would like to change some details, you can still call up the different configuration pages via your menu. This is especially useful with regard to the "Technical Information" page since 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. You can complete the form with fake details in the test environment. However, in the production environment, you have to fill in the correct affiliation details with 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 link "Payment methods" in your

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'll see a reference to the related items in the Technical Information page or to your website, depending on where you need to take action.

You can access the technical parameters via the link "Technical Information" 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 in your "Technical Information" page, which represents 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 described here: Sale Process. After you have performed a transaction, you can view the details in the back-office of your account. When you're logged in, click the "View transactions" link in your menu, enter your selection criteria (the first time, enable all the status checkboxes 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.

Ref	Merch ref	Orders (dd/mm/yyyy)	Status ?	Autor.	Payments (dd/mm/yyyy)	Total	Name	Method
1371176	order0021	12/09/2006 11:22:16	5-Authorized	testoff	0	75.10 EUR	Jack Smith	MasterCard
1371351	test1	12/09/2006 14:49:41	0-Invalid or incomplete		0	1.00 EUR	Bill Smith	CreditCard
1371518	Order7	12/09/2006 15:59:38	9-Payment requested	testoff	12/09/2006	345.00 EUR	Jack Russel	VISA

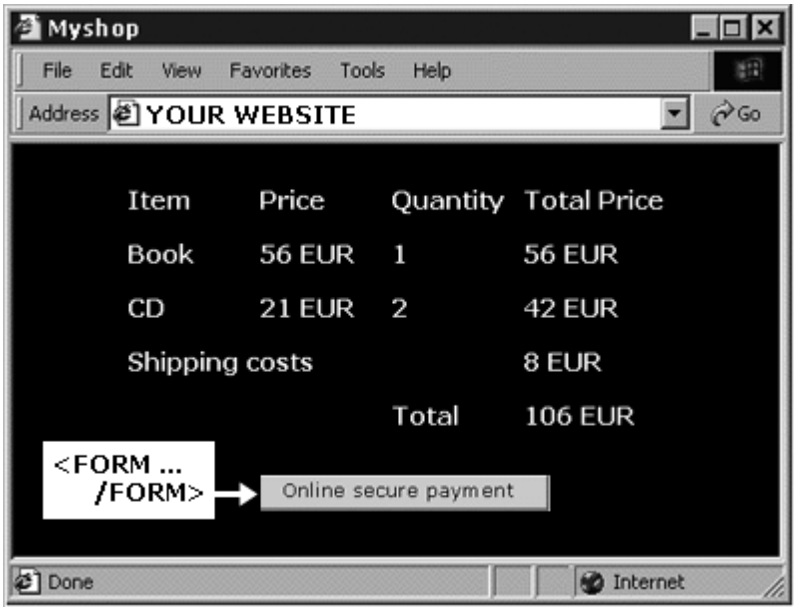
The most frequent transaction statuses are:

0 - Incomplete or invalid
1 - Cancelled by client
2 - Authorization refused
5 - Authorized
9 - Payment requested

More information about the different transaction statuses can be found at: https://secure.ogone.com/ncol/paymentinfos1.asp

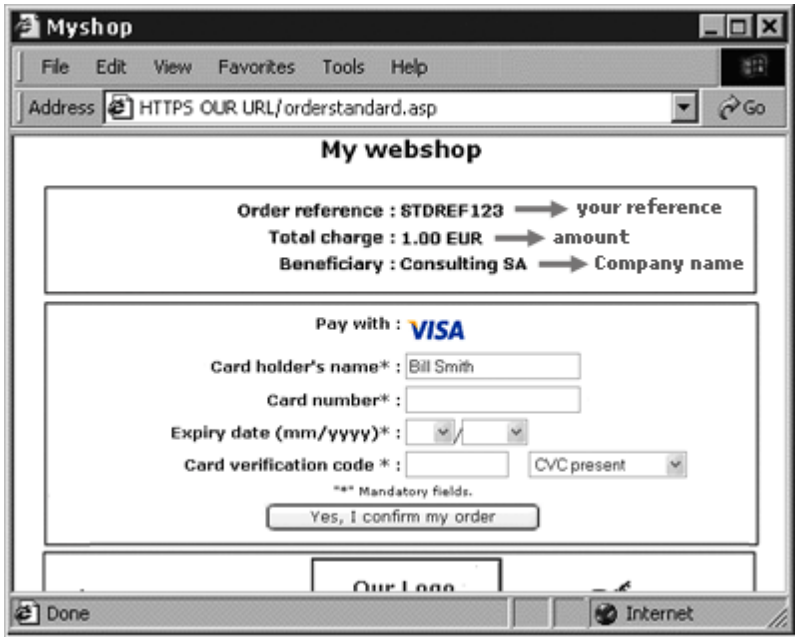
3 Sale Process

The following screenshots represent a sale process after the 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 here: Link between the Merchant's Website and our Payment Page.



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

If payment is by credit card, the customer will be requested to enter his card number, etc. 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 has been refused, an error is shown and the customer has the possibility to retry: he can choose another payment method or change the details he had 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 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 that last page. Following is the block of code you need to paste in the last page of your shopping basket:

```
<form method="post" action="https://secure.ogone.com/ncol/XXXX/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 also send us the customer name, customer's e-mail, address, town, zip, country and telephone number since they can be useful tools for combating fraud.

Following is 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. For instance: EUR, USD, GBP, …
language	Language of the customer. For instance: en_US, nl_NL, fr_FR, …
CN	Customer name. Will be pre-initialized (but still editable) in the Customer Name field of the credit card details.
EMAIL	Customer's e-mail address
owneraddress	Customer's street name and number
ownerZIP	Customer's ZIP code
ownertown	Customer's town/city name
ownercty	Customer's country
ownertelno	Customer's telephone number

For more technical details about these fields, please refer to the online 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 the "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.

5 Security: Check before the Payment

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

5.1 Referrer

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

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

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

If you enter a wrong URL, you'll see the error "*unknown order/1/r*" on the payment page.

5.2 SHA-IN signature

Because the referrer check is not foolproof, our system can perform a data check before processing the payment to ensure the accuracy and integrity of the order data. This data check is not mandatory, but highly recommended. If you don't use it, you will not be allowed to configure "Sale" as default operation code or an automatic data capture by our system as default data capture (payment) procedure in your account in (see General Payment Parameters), you will have to use a 2 phase – authorization followed by a manual data capture (payment request) – procedure for credit card transactions.

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.

IMPORTANT: If you are unable to integrate this, but don't wish to use a manual, two step procedure for credit card payments, you can send us a signed fax to request us to disable this data check for you. This means, however, that *you* take responsibility for the correctness of the order data and their integrity in the redirection process.

5.2.1 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'), separated by a passphrase. The passphrase is defined in the Merchant's *Technical information*, 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 Appendix 1: List of Parameters to be included in SHA Calculations), will be included in the string to hash.
- all parameter names should be in UPPERCASE (to avoid any case confusion)
- all parameters need to be put alphabetically
- parameters that do not have a value should NOT be included in the string to hash

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 at https://secure.ogone.com/ncol/test/testsha.asp

Example of a basic SHA-1-IN calculation

parameters (in alphabetical order)
amount: 15.00 -> 1500
currency: EUR
Operation: RES
orderID: 1234
PSPID: MyPSPID

SHA Passphrase (In technical info)
Mysecretsig1875!?

string to hash
AMOUNT=1500Mysecretsig1875!?CURRENCY=EURMysecretsig1875!?
OPERATION=RESMysecretsig1875!?ORDERID=1234Mysecretsig1875!?
PSPID=MyPSPIDMysecretsig1875!?

resulting Digest (SHA-1)
EB52902BCC4B50DC1250E5A7C1068ECF97751256

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/pass phrase) entered in the SHA-1-IN Signature field in the "Data and origin verification" tab, "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/pass phrase) has been entered in the SHA-1-IN Signature field in the "Data and origin verification" tab, "Checks for e-Commerce" section of the Technical Information page – indicating you want to use a 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.

5.2.2 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. If you work in a windows 2000/asp environment, you can download a DLL that includes a method to hash a string using SHA-1 in the Support > Documentation page.

Because there are many possible combinations of operating systems (version-numbers/patches) and programming languages we cannot be held responsible for any errors on your server during installation and/or processing.

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

6 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 customize our static template.

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

Following are 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 color	white
TXTCOLOR	Text color	black
TBLBGCOLOR	Table background color	white
TBLTXTCOLOR	Table text color	black
BUTTONBGCOLOR	Button background color	_
BUTTONTXTCOLOR	Button text color	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 a JPG or GIF file (and your PSPID) to support@ogone.com (only for production accounts. Please make sure the "Logo Hosting" option is active in your Account > Options page before sending us your logo). If the logo is stored on our servers, you only need to enter the filename, not the whole URL.	_

For more technical details about these fields, please refer to the online Parameter Cookbook.

The colours can be specified by their hexadecimal code (#FFFFFF) or their name (white). First check 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 an advanced integration. You can find more information on this in the **Advanced e-Commerce Integration Guide**.

7 Transaction Feedback to the Customer

Where to configure? Your website (shopping basket), Technical Information – Transaction e-mails tab – E-mails to the customer

7.1 On screen

If you don't specify anything, our system shows the customer a standard message: "Your payment is authorised" 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 4 URLs (accepturl, exceptionurl, cancelurl and declineurl) where our system redirects the customer 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 authorized (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 declines the authorisation (status 2) more than 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 shown 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 declineurl will be shown to the customer instead.

*For more technical details about these fields, please refer to the online **Parameter Cookbook**.*

You can also configure these URLs in the "Transaction feedback" tab, "HTTP redirection in the browser" section of the Technical Information page.

7.2 By e-mail

Our system can send an automatic e-mail to your customer notifying him of the transaction registration. This is a standard e-mail whose contents you cannot change. You can activate this option in the "Transaction e-mails" tab, "E-mails to the customer" section of the Technical Information page.

7.3 Other (Advanced)

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

8 Transaction Feedback to the Merchant

Where to configure? Your website (database), Technical Information – Transaction e-mails tab – E-mails to the merchant section, Technical Information – Transaction feedback tab – HTTP redirection in the browser section

8.1 Back-office

You can always view the transaction results in the back-office of your account. When you're logged in, click the "Financial History" link or the "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.

8.2 By e-mail

You can receive a payment confirmation e-mail from our system for each transaction (option to configure in the "Transaction e-mails" tab, "E-mails to the merchant" section of the Technical Information page).

8.3 Request on your page

When a payment is executed, we can send the following parameter list in a request on your accept-, exception-, cancel- or declineurl to enable you to perform a database update:

Parameter	**Value**
orderID	Your order reference
amount	Order amount (not multiplied by 100)
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
NC ERROR	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-1-OUT configured by you.

You can activate this option in the "Transaction feedback" tab, "HTTP redirection in the browser" section of the Technical Information page ("I would like to receive transaction feedback parameters on the redirection URLs").

IMPORTANT: You need to use a SHA signature to verify the request contents when you use this option, to prevent customers tampering with details in the URL field to cause an incorrect database update. If you do not configure a SHA-1-OUT signature we will not send any parameters on your accept-, exception-, cancel- or declineurl.

This string is constructed by concatenating the values of the fields sent with the order (sorted alphabetically, in the format 'parameter=value'), separated by a passphrase. The passphrase is defined in the Merchant's *Technical information*, under the tab "Transaction Feedback", section "All transaction Submission modes." For the full list of parameters to include in the SHA Digest, please refer to Appendix 1. Please note that these values are all case sensitive.

Important: all parameter names should be in UPPERCASE (to avoid any case confusion)

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 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.

Example of a basic SHA-1-OUT calculation

ACCEPTANCE: 1234
amount: 15
BRAND: VISA
CARDNO: xxxxxxxxxxxx1111
currency: EUR
NCERROR: 0
orderID: 12
PAYID: 32100123
PM: CreditCard
STATUS: 9

additional string: Mysecretsig1875!?

Entire string to be hashed:
ACCEPTANCE=1234Mysecretsig1875!?AMOUNT=1500Mysecretsig1875!?
BRAND=VISAMysecretsig1875!?CARDNO=xxxxxxxxxxxx1111Mysecretsig1875!?
CURRENCY=EURMysecretsig1875!?NCERROR=0Mysecretsig1875!?
ORDERID=12Mysecretsig1875!?PAYID=32100123Mysecretsig1875!?
PM=CreditCardMysecretsig1875!?STATUS=9Mysecretsig1875!?

Resulting Digest (SHA-1):
28B64901DF2528AD100609163BDF73E3EF92F3D4

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

8.4 Other (Advanced)

It is also possible to receive a request with transaction parameters from our end on a specific page at your end that 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**.

9 General Payment Parameters

IMPORTANT: This chapter is only applicable for payment methods such as credit cards that allow you to reserve the customer's money without charging him 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

9.1 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 or the account, or the request is matched against a blacklist. In the data capture (payment request) step, your acquirer is requested to take the reserved or blacklist-matched amount on the customer's card or 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 on the customer's account until a data capture (payment request) has been performed).
- **Sale**: our system automatically requests the payment (transfer of the amount) immediately after a 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, a data capture will have to be performed on the transaction 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.

9.2 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 authorize offline processing in those 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. (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 since 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.

10 Appendix 1: List of Parameters to be included in SHA Calculations

10.1 SHA-IN

ACCEPTURL
ADDMATCH
ADDRMATCH
AIAIRNAME
AIAIRTAX
AIBOOKIND*XX*
AICARRIER*XX*
AICHDET
AICLASS*XX*
AICONJTI
AIDESTCITY*XX*
AIDESTCITYL*XX*
AIEXTRAPASNAME*XX*
AIEYCD
AIFLDATE*XX*
AIFLNUM*XX*
AIIRST
AIORCITY*XX*
AIORCITYL*XX*
AIPASNAME
AISTOPOV*XX*
AITIDATE
AITINUM
AITYPCH
AIVATAMNT
AIVATAPPL
ALIAS
ALIASOPERATION
ALIASUSAGE
ALLOWCORRECTION
AMOUNT
AMOUNT*XX*
AMOUNTHTVA
AMOUNTTVA
BACKURL
BGCOLOR
BRAND
BRANDVISUAL
BUTTONBGCOLOR
BUTTONTXTCOLOR
CANCELURL
CARDNO
CATALOGURL
CAVV_3D
CAVVALGORITHM_3D
CERTID
CHECK_AAV
CIVILITY
CN
COM
COMPLUS
COSTCENTER
COSTCODE
CREDITCODE
CUID
CURRENCY
CVC
DATA
DATATYPE
DATEIN
DATEOUT

DECLINEURL
DISCOUNTRATE
ECI
ECOM_BILLTO_POSTAL_CITY
ECOM_BILLTO_POSTAL_COUNTRYCODE
ECOM_BILLTO_POSTAL_NAME_FIRST
ECOM_BILLTO_POSTAL_NAME_LAST
ECOM_BILLTO_POSTAL_POSTALCODE
ECOM_BILLTO_POSTAL_STREET_LINE1
ECOM_BILLTO_POSTAL_STREET_LINE2
ECOM_BILLTO_POSTAL_STREET_NUMBER
ECOM_CONSUMERID
ECOM_CONSUMERORDERID
ECOM_CONSUMERUSERALIAS
ECOM_PAYMENT_CARD_EXPDATE_MONTH
ECOM_PAYMENT_CARD_EXPDATE_YEAR
ECOM_PAYMENT_CARD_NAME
ECOM_PAYMENT_CARD_VERIFICATION
ECOM_SHIPTO_COMPANY
ECOM_SHIPTO_DOB
ECOM_SHIPTO_ONLINE_EMAIL
ECOM_SHIPTO_POSTAL_CITY
ECOM_SHIPTO_POSTAL_COUNTRYCODE
ECOM_SHIPTO_POSTAL_NAME_FIRST
ECOM_SHIPTO_POSTAL_NAME_LAST
ECOM_SHIPTO_POSTAL_POSTALCODE
ECOM_SHIPTO_POSTAL_STREET_LINE1
ECOM_SHIPTO_POSTAL_STREET_LINE2
ECOM_SHIPTO_POSTAL_STREET_NUMBER
ECOM_SHIPTO_TELECOM_FAX_NUMBER
ECOM_SHIPTO_TELECOM_PHONE_NUMBER
ECOM_SHIPTO_TVA
ED
EMAIL
EXCEPTIONURL
EXCLPMLIST
EXECUTIONDATE*XX*
FIRSTCALL
FLAG3D
FONTTYPE
FORCECODE1
FORCECODE2
FORCECODEHASH
FORCEPROCESS
FORCETP
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
INVDATE
INVDISCOUNT
INVLEVEL
INVORDERID
ISSUERID
ITEMCATEGORY*XX*
ITEMDISCOUNT*XX*
ITEMID*XX*
ITEMNAME*XX*
ITEMPRICE*XX*

ITEMQUANT*XX*
ITEMUNITOFMEASURE*XX*
ITEMVATCODE*XX*
LANGUAGE
LEVEL1AUTHCPC
LIDEXCL*XX*
LIMITCLIENTSCRIPTUSAGE
LINE_REF
LIST_BIN
LIST_COUNTRIES
LOGO
MERCHANTID
MODE
MTIME
MVER
NETAMOUNT
OPERATION
ORDERID
ORIG
OR_INVORDERID
OR_ORDERID
OWNERADDRESS
OWNERADDRESS2
OWNERCTY
OWNERTELNO
OWNERTOWN
OWNERZIP
PAIDAMOUNT
PARAMPLUS
PARAMVAR
PAYID
PAYMETHOD
PM
PMLIST
PMLISTPMLISTTYPE
PMLISTTYPE
PMLISTTYPEPMLIST
PMTYPE
POPUP
POST
PSPID
PSWD
REF
REFER
REFID
REFKIND
REF_CUSTOMERID
REF_CUSTOMERREF
REMOTE_ADDR
REQGENFIELDS
RTIMEOUT
RTIMEOUTREQUESTEDTIMEOUT
SCORINGCLIENT
SETT_BATCH
SID
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
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

10.2SHA-OUT

AAVADDRESS
AAVCHECK
AAVZIP
ACCEPTANCE
ALIAS
AMOUNT
BRAND
CARDNO
CCCTY
CN
COMPLUS
CREATION_STATUS
CURRENCY
CVCCHECK
DCC_COMMPERCENTAGE
DCC_CONVAMOUNT
DCC_CONVCCY
DCC_EXCHRATE
DCC_EXCHRATESOURCE
DCC_EXCHRATETS
DCC_INDICATOR
DCC_MARGINPERCENTAGE
DCC_VALIDHOURS
DIGESTCARDNO
ECI
ED
ENCCARDNO
IP
IPCTY
NBREMAILUSAGE
NBRIPUSAGE
NBRIPUSAGE_ALLTX
NBRUSAGE
NCERROR
ORDERID
PAYID

PM
SCO_CATEGORY
SCORING
STATUS
SUBSCRIPTION_ID
TRXDATE
VC