



# **SKYPAY *COMPLETE* INTEGRATION GUIDE**

## Table of Contents

Introduction.....	3
Process Overview.....	4
Transaction Registration.....	5
Action.....	5
Response.....	6
POST to payment URL.....	8
Request.....	8
Callback response.....	9
Response.....	9
Appendix A – Currency Codes.....	11
Appendix B – Line Item Detail.....	12
Appendix C – AVS/CVV.....	13

## Introduction

The *Skypay Complete* solution allows merchants to transact cards online from their website securely and compliantly without having to implement their own 3DSecure and secure payment facility. By offloading the payment responsibility to the Skypay system merchants can avoid the potentially large costs surrounding PCI DSS compliance testing.

Skypay undergo an annual onsite audit to ensure the highest levels of card processing compliance to give complete peace of mind to our customers.

The system uses a secure registration and processing methodology that makes it impossible to interfere with the key transaction information that some older cart and payment systems permit. We use secure encryption algorithms throughout while keeping the system simple and intuitive to use.

## Process Overview

The Skypay Complete method of integration consists of up to four phases:

1. Registration
2. Payment form
3. 3DSecure authentication\*
4. Notification

*\* Optional stage dependent on cardholder enrolment status and merchant account status.*

The registration phase consists of a HTTPS POST request to the Skypay system to register the key components of the transaction behind the scenes. This replaces traditional systems where this information was passed during the redirection to the payment form and makes it considerably more secure. The transmitted data is validated and checked for syntax and a response is returned that contains an ID for the transaction and an encrypted data block.

Once registration is complete the user is redirected to the secure payment form on the Skypay system sending the ID and encrypted block as POST data once again. The payment form will then retrieve the details of the transaction and display them for the cardholder with fields for entering the sensitive card information.

When the user submits their payment, and if you are signed up for 3DSecure processing, the user's card data is checked against bank records to see if they have enrolled in the 3DSecure schemes of Mastercard SecureCode or Verified by VISA. If they are then the system will redirect the user to the corresponding authentication form at their bank and they will be prompted for a password or other data to prove their identity.

Upon submission of the payment form or subsequent authentication form for 3DSecure the payment is sent to the bank for authorisation. If there was a failure or they did not pass authentication the form will display an error stating the reason and allow for another attempt. If however the payment was successful then the user is redirected to the page that was specified in SuccessURL during registration. Before the redirect occurs the system will also send a background request to the CallbackURL containing status information about the transaction and also any additional fields that were requested in the CallbackArgs parameter. This allows your site to update its order status securely without tampering and this URL can be secured to only permit access from Skypay.

## Transaction Registration

### Action

Your payment solution must first register its intent to make a payment using our transaction registration system. This occurs as a background process using a POST request and SSL encryption to ensure that the parameters such as the payment amount cannot be tampered with externally.

The fields that can be supplied are detailed below with optional arguments marked with an \*.

Field Name	Data Type	Description
Username	V	Username for payment API
Password	V	Password for payment API
TestMode	N [1 or 0]	If set to 1 the system will process in Testing mode and only test card details will operate.
Dispatch	N [1 or 0]	Take the payment 1 = NOW or just pre-authenticate the card for 0 = LATER processing. The default is NOW (1). ** This is the reverse of the earlier setup **
DispatchAmount*	N	When using LATER processing this determines the value that will be pre-authenticated.
Amount	N	The amount of the transaction to be charged in minor units e.g. pence
Description	V	A description of the order **previously Order**
CardName	V	The Name of the cardholder
CardAddress	V	The Address of the cardholder
CardPostcode	V	The Postcode of the cardholder
Telephone*	V	The Telephone number of the purchaser
Email*	V	The Email of the purchaser
CurrencyCode	N	The Currency that the transaction will be taken using. You will need to pre-arrange this with your bank. The default value is 826 for GBP
OrderID*	N	An optional Order ID for this transaction, useful for later searching if your system has a unique value already.
CustomerID*	N	An optional Customer ID for this transaction, useful for later searching if you store a unique reference already. **for card selection services this must be provided**
AVSCV2Check	N [1 or 0]	Perform checks on the Address and CVV number on the card. The default is no (0).

3DSecureCheck	N [1 or 0 or 2]	Perform 3DSecure validation on the order if the cardholder is enrolled. You must have this feature enabled on your account for it to work. The default is no (0). If set to 2 then the system will also fail any transactions for which enrolment could not be checked.
StoreCard*	N [1 or 0]	Store the card information for processing later. You will need to register to use this facility and will be issued a card storage key that must be updated every 12 months. The default is no (0)
CardPassphrase*	V	When StoreCard is set to "1" this parameter is required and represents your card storage passphrase. Please contact us if you require this facility.
CallbackURL	V	The URL of your secure callback script to which we will send notifications of payment success.
SuccessURL	V	The URL of the page to which a user will be directed if they pay successfully.
AbortURL	V	The URL of the page that the user will be sent to if they opt to cancel the payment. Typically the checkout page on your website.
FormTemplate*	V	If using a customised payment template then this may be specified here to display the branded copy rather than the default. You will need to register to use this service.
CallbackArgs*	V	This is a list of key=value pairs separated by & characters much like in a URL listing the fields that will be POSTed back to your callback URL on a successful transaction. Useful for sending your own sessionID or unique reference so you can tie a payment to a transaction.

All of this data should be POSTed to our secure registration URL at <https://secure.skypay.co.uk/api/transactionRegister.cgi> and must be properly URL encoded. If your HTTP extension does not automatically encode transmitted data then you will need to do this manually first.

Registration attempts that are left unused will time out after 1 hour and be removed from the system. This will result in an error being displayed if someone then attempts to pay with it so you should ensure that the registration is only performed at the point where the user is given the option to redirect to the payment form.

The result of the POST is returned directly as a list of parameter=value responses, one per line:

## **Response**

Field Name	Field Type	Description
Result	OK or ERROR	An indicator to show whether the transaction registration was successful or not.
PaymentURL	V	The URL of the payment form to which you should direct

		the user to enter their card details. This should be a POST request using a form (see section 2).
TransactionID	N	A unique ID identifying this transaction attempt which should be sent to the payment form in stage 2.
TransactionKey	V	A string containing a hash that is unique to your transaction request. This should be retained as you can then use it to validate the callback after a successful transaction for added security.
EncBlock	V	An text field containing an encrypted block of data required for payment processing at the next stage. ** replaces the encryption keys of the earlier version and relieves the necessity for client side encryption **
ErrNum	V	In the event of an error this will contain an error number identifying the cause. You can report this code to us with the ErrStr value if you need assistance with the error.
ErrStr	V	In the event of an error this will contain a description of the problem to help you diagnose the fault.

The TransactionID value may be stored for reference purposes if desired though you should **not** store the EncBlock data at any stage as it is not relevant beyond the scope of the transaction.

In the event of an error you will find an error number and description in the ErrNum and ErrStr response parameters. If you have difficulty interpreting the error please contact support who will be able to advise you.

## POST to payment URL

After successful registration it is now possible to direct the purchaser to the secure payment form for entry of their card information. This is achieved by producing a simple confirmation form or self submitting form that sends the following parameters to the payment URL.

The form method should be set as POST and the form action should be set as the full text received from the registration request in step 1.

### *Request*

Field Name	Field Type	Description
transactionID	N	The numerical transaction ID returned by transaction registration.
encBlock	V	The encrypted block of data returned by the registration phase.

In OSCommerce this is typically achieved using the payment button code at the confirmation stage of the checkout though you may wish to use a self submitting form to achieve this in bespoke applications.

## Callback response

Following a successful payment the user will be redirected to the supplied success URL. Immediately prior to this a call will be made to the supplied callback URL providing the result detail of the payment to be stored in your records.

In addition to the fields listed below we will also pass back each parameter from the CallbackArgs field and the corresponding value that was specified during the registration phase.

### Response

Field Name	Field Value	Description
Authcode	V	The authorisation code provided by the payee acquirer.
CrossRef	N	A unique numerical reference for the transaction. This is useful for tracking the transaction later. ** replaces Twincheck from the earlier implementations **
CVVResponseText	V	A readable result from the AVS and CVV checks if performed.
CardID	N	The ID of the credit card if card storage is enabled. You can use this with your card storage key in lieu of the card details for later processing if enabled.
Result	V	This should always be SUCCESS for the callback.
TransactionKey	V	A string containing a hash that is unique to the transaction. Compare this with the one given at registration to ensure the callback is valid.
TDSEnrolled	V	Indicated whether the payee was 3DSecure enrolled if enabled.
TDSAuthenticated	V	Indicates whether the payee authenticated using 3DSecure if enabled.
TDSTransactionID	N	A unique transaction reference specific to the 3DSecure check if enabled.
TDSECI	N	The 3DSecure ECI parameter returned by 3dSecure authentication if enabled.
TDSCAVV	V	The 3DSecure CAVV parameter returned by 3DSecure authentication if enabled.
TDSErrorCode	V	The 3DSecure error code if the process was not successful.
TDSErrorDescription	V	A description of the 3DSecure error if the process was not successful.
TDSiReqCode	V	Additional 3DSecure error information returned by some issuers.
TDSiReqDetail	V	Additional 3DSecure error information returned by some issuers.
TestMode	N [0 or 1]	If the transaction was set in TestMode during registration then this will be set to "1" so that you can identify tests and deal with them

		appropriately.
--	--	----------------

Note: If 3DSecure checks are enabled on your account then you should always store all of the 3Dsecure response parameters with each transaction. This will enable you to defend any chargeback requests that may arise and help ensure that any financial risk is with the bank.

Any additional fields that you specified in the CallbackArgs parameter at registration will be transmitted along side these common fields. Please note that if you have duplicated any of the names used above they will be overwritten with the values that we generate.

You should **not** need to transmit any sensitive parameters in the callback request as your system can store these and use an order reference or session to retrieve them from the callback.

## Appendix A – Currency Codes

The Skypay system supports any currency that is described in ISO-4217 which are the 3-digit numerical identifiers.

It is essential that you obtain clearance from your acquiring bank (acquirer) before you attempt to use multi-currency transactions. Certain acquirers will insist that you use separate Internet merchant account numbers for each currency and some banks will not allow all currencies.

Once you have obtained clearance from your bank you may then choose from one of the common currency codes below. If you have been provided with a separate merchant account number for your new currency, please send this to our support team with the currency that you will be using it for and we can have the account activated for you.

<b>Currency</b>	<b>ISO-4217 Code</b>
Australian Dollar	36
Canadian Dollar	124
Czech Koruna	203
Danish Krone	208
Hong Kong Dollars	344
Icelandic Krona	352
Japanese Yen	392
Norwegian Krone	578
Singapore Dollar	702
Swedish Krona	752
Swiss Franc	756
Pound Sterling	826
US Dollar	840
Euro	978

## Appendix B – Line Item Detail

If you plan to support either Amex or VISA purchasing cards you will be required to transmit further information about your transaction at the registration stage. This includes separate information for up to six items, containing a description, quantity and gross value. This is used by the card issuer to scrutinise payments and give a breakdown of payments on the owner's statement.

Field Name	Field Value	Description
LIDItemXDescription	V [max 15 chars]	A short description of the item
LIDItemXQuantity	N [1 - 999]	The quantity of the item that was ordered
LIDItemXGrossValue	N [1 - 9999999999]	The gross value of the item in minor units e.g. pence.

You can supply up to 6 line items for any given sale and you should replace the X in the field names above with a value of 1 through 6 to indicate the item number.

## Appendix C – AVS/CVV

The Skypay system supports both AVS (Address Verification) and CVV (Card Verification Value) checking to aid with fraud screening.

If you supplied a value of “1” to the AVSCV2Check parameter during transaction registration we will attempt to perform this check on your payment. It is vital that you send to us what has been supplied as the card holders address and postal code in order to get accurate results.

It is possible to make these checks on VISA, Mastercard/Europay, Maestro and American Express cards, but only those registered in the UK as the standard is not unified globally.

The results of the test will be supplied as part of the Callback request upon a successful authorisation and is passed in the parameter CVVResponseText. Possible responses are as follows:

<b>Response Message</b>	<b>Description</b>
ALL MATCH	AVS and CVV match
SECURITY CODE MATCH ONLY	CVV value matched but address/postcode did not
ADDRESS MATCH ONLY	Address and postcode matched but CVV did not
NO DATA MATCHES	Neither Address/Postcode or CVV matched
SECURITY CHECKS NOT SUPPORTED	Card scheme does not support checks
UNKNOWN RESPONSE	An unrecognised response was received