



**eSec HTTP Post
Integration Guide**

Table of Contents

1	Introduction	3
1.1	About this Guide	3
1.2	Intended Audience	3
1.3	System Overview	3
2	Payment Gateway Integration	4
2.1	Direct Model	4
2.2	Using the Integration Interface.....	4
3	Transaction Parameters	5
4	Parameter Formats	9
4.1	Response Fields.....	9

1 Introduction

1.1 About this Guide

This guide provides technical information about integrating and configuring eSec within your environment.

1.2 Intended Audience

This document is intended for developers, integrating eSec into their own applications or websites.

1.3 System Overview

eSec's Internet payment gateway is a secure method for authorising credit card transactions over the Internet.

Used by merchants as a means for customers to pay for goods and services on a Web site via a shopping cart, the Payment Gateway can also be utilised for merchant applications, such as bulk payments, and for integration with corporate databases, accounting packages, and even interactive voice recognition systems.

The Payment Gateway is easy to integrate with any application or Web site and supports major credit cards. This gateway service was designed with security in mind - information is disseminated on a "need to know" basis to participants in the transaction. Client credit card details are encrypted the moment that they are transmitted by the client to the banking network.

SecurePay partners with the following major banks and financial institutions in the provision of the eSec Payments Gateway:

- ANZ
- American Express
- BankWest
- Commonwealth Bank
- Diners Club
- National Australia Bank
- St George (including Bank of SA)
- Westpac (including Challenge Bank and Bank of Melbourne)

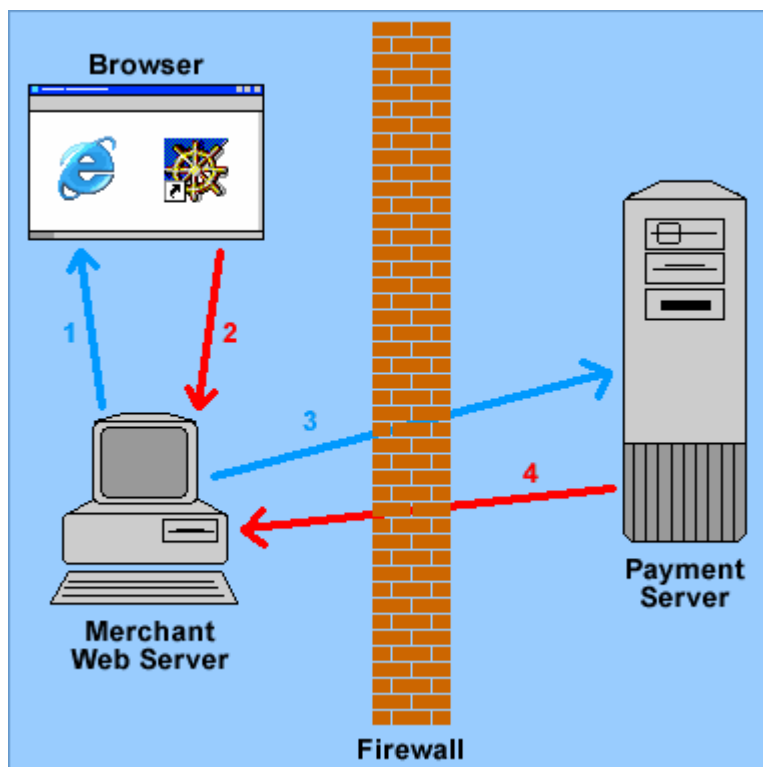
2 Payment Gateway Integration

Payment Gateway Integration Interface is intended to be driven by an application via an SSL-encrypted HTTP connection to a CGI program. The data for the transaction is passed to the service using the standard format for either an HTTP POST or GET request.

The Payment Gateway Integration Interface utilises the [Direct Model](#) for transaction management.

2.1 Direct Model

The Direct Model for the Payment Gateway interfaces allows the merchant to integrate payments directly into their own business system as a backend service. This model provides the greatest level of control and is intended for use by merchants that perform some form of processing on transactions before submitting the request, or for merchants that utilise a store-and-forward method of processing transactions.



2.2 Using the Integration Interface

The parameters to the CGI program provide the Payment Gateway Integration Interface with the information needed to correctly transmit the transaction request to the Payment Gateway for processing. These parameters, as noted below, must be provided by the merchant's processing system. Unless otherwise noted by eSec, these parameters should be entered exactly as given with no modifications; otherwise the Payment Gateway may not function correctly.

The URL of the CGI program to be invoked to establish the connection to the Payment Gateway is as follows:

<https://sec.aba.net.au/cgi-bin/service/authint>

3 Transaction Parameters

<p>EPS_MERCHANT</p>	<p>An unique identifier for the merchant within the Payment Gateway. This merchant identifier value is an alphanumeric string allocated to the merchant by eSec, although for testing purposes an identifier value of "test" may be used. This merchant identifier value is not the same as the merchant agreement number given to the merchant by an acquiring financial institution.</p> <p>Examples:</p> <pre><input type="HIDDEN" name="EPS_MERCHANT" value="test"> <input type="HIDDEN" name="EPS_MERCHANT" value="widgetsrus"></pre>
<p>EPS_REFERENCEID</p>	<p>An alphanumeric string that allows the merchant's processing system to identify an individual transaction. The format of this string is of no importance to the Payment Gateway, since the value is simply stored by the Payment Gateway as part of the transaction record and returned to the merchant's processing system in the transaction result.</p> <p>Examples:</p> <pre><INPUT TYPE="HIDDEN" NAME="EPS_REFERENCEID" VALUE="1234567890"> <INPUT TYPE="HIDDEN" NAME="EPS_REFERENCEID" VALUE="20010410-123456"></pre>
<p>EPS_CARDNUMBER</p>	<p>The number from the credit card to be used for the purchase. This number must be greater than 12 digits, less than 19 digits and must conform to the credit card checkdigit scheme. Spaces and hyphens included in the card number value will be removed before processing.</p> <p>When sending transactions to the Payment Gateway test facility, and only to the test facility, the following special card "numbers" may be submitted:</p> <ul style="list-style-type: none"> • testsuccess - Always successfully processed and authorised • testfailure - Always successfully processed and refused • testtimeout - Never responds and the transaction will time out <p>The test facility does not normally accept real credit card numbers, however additional test facilities may be made available under certain specific exceptional circumstances. The Payment Gateway live facility will not accept the test card numbers listed above under any circumstances.</p> <p>Examples:</p> <pre><INPUT TYPE="HIDDEN" NAME="EPS_CARDNUMBER" VALUE="testsuccess"> <INPUT TYPE="HIDDEN" NAME="EPS_CARDNUMBER" VALUE="1234567890123456"></pre>
<p>EPS_CARDTYPE</p>	<p>A string containing the name of the credit card issuer that provided the credit card. This may currently be one of the strings "visa", "mastercard", "bankcard", "amex", "dinersclub" or "jcb" in any mixture of case. If this parameter is not correctly set to one of the values listed above, the transaction will be rejected.</p> <p>When sending transactions to the Payment Gateway test facility, and only to the test facility, the special card type "testcard" should be used to identify the special test card numbers listed above. Failure to set the card type field to "testcard" when sending test card numbers will cause the Payment Gateway to reject the transaction.</p> <p>Examples:</p>

	<p><INPUT TYPE="HIDDEN" NAME="EPS_CARDTYPE" VALUE="testcard"></p> <p><INPUT TYPE="HIDDEN" NAME="EPS_CARDTYPE" VALUE="visa"></p>
EPS_EXPIRYMONTH	<p>The month in which the credit card expires. This may only contain an integer value between 1 and 12, inclusive, corresponding to the month of the year.</p> <p>The expiry month and expiry year together must form a date that is at least the current month. Transactions that contain an expiry date in the past will be rejected.</p> <p>Examples:</p> <p><INPUT TYPE="HIDDEN" NAME="EPS_EXPIRYMONTH" VALUE="1"></p> <p><INPUT TYPE="HIDDEN" NAME="EPS_EXPIRYMONTH" VALUE="12"></p>
EPS_EXPIRYYEAR	<p>The year in which the credit card expires. This should ideally be a full 4 digit year value to remove any possible ambiguity, however if a two digit year is provided, the Payment Gateway will assume that a value of "99" refers to 1999 and that any other value refers to a value of "20XX", where XX is the 2 digit value provided. The expiry month and expiry year together must form a date that is at least the current month. Transactions that contain an expiry date in the past will be rejected. It is strongly recommended that a full 4 digit year be specified as the value of this parameter since support for two digit years will be withdrawn in a future release of this interface.</p> <p>Examples:</p> <p><input type="HIDDEN" name="EPS_EXPIRYYEAR" value="2001"></p> <p><input type="HIDDEN" name="EPS_EXPIRYYEAR" value="01"></p>
EPS_NAMEONCARD	<p>The card holder's name as specified on the credit card. This parameter must contain a non-null alphabetic string of up to 50 characters.</p> <p>Examples:</p> <p><input type="HIDDEN" name="EPS_NAMEONCARD" value="John A. Citizen"></p> <p><input type="HIDDEN" name="EPS_NAMEONCARD" value="Jane M. Person"></p>
EPS_AMOUNT	<p>The total amount of the purchase transaction. This value may be specified either as a decimal dollar amount (in which case there MUST be two digits after the decimal place) or as a value in cents. If a decimal point is not included in the amount value, then the amount is assumed to be a value in cents. Please be careful to correctly specify the amount as the Payment Gateway has no way of determining whether an amount has been correctly specified. As an example, assume a transaction is being submitted for an amount of AUD\$107.95. This amount may be submitted to the Payment Gateway in either of the following forms:</p> <p><input type="HIDDEN" name="EPS_AMOUNT" value="10795"></p> <p><input type="HIDDEN" name="EPS_AMOUNT" value="107.95"></p> <p>The first form above indicates a value of 10795 cents, which is the preferred method for submitting amounts. Using the minor currency unit (i.e. cents) allows for easier expansion into future multi-currency services. Be very careful to ensure that amounts in whole dollars, i.e. with only zeros after the decimal point, are submitted <i>*with the trailing zeros intact*</i>. If an amount such as AUD\$107.00 is simply submitted as 107, the Payment Gateway will assume that this is 107 <i>*cents*</i> and will process the transactions as such. The correct form for an amount such as this one is either of "10700" or "107.00".</p> <p>Null or zero and negative amounts are not acceptable and transactions containing such</p>

	amount values will be rejected.
EPS_CCV	<p>The Card Check Value (CCV) field should contain a three or four digit value that is printed on the back of the credit card itself. If the CCV value is not available, either because it is not present on the card (some cards still do not have CCV values printed on them), or because the card holder does not wish to enter it, this field should be left empty.</p> <p>When sending transactions to the Payment Gateway test facility, and only to the test facility, CCV values of "1234" and "999" are accepted as valid fields. The CCV field may also be left empty for testing.</p> <p>This field may be referred to elsewhere as a Card Verification Value (CVV) or a Card Verification Code (CVC), most notably in information provided by banks or credit card providers.</p> <p>Examples:</p> <pre><input type="HIDDEN" name="EPS_CCV" value="1234"> <input type="HIDDEN" name="EPS_CCV" value="999"></pre>
EPS_VERSION	<p>An integer that specifies the SSL Web Interface Specification response version that the merchant's processing system requires. This may take a value of 1, 2, 3, or 4, for a response in the required format. The differences between the response versions are described later in this document. If not set to any value, the Payment Gateway assumes a Version 1 response.</p> <p>Examples:</p> <pre><input type="HIDDEN" name="EPS_VERSION" value="1"> <input type="HIDDEN" name="EPS_VERSION" value="2"></pre>
EPS_TEST	<p>A boolean field that specifies whether the transaction should be sent to the Payment Gateway's test facility. If this element exists and contains a value of "true", the transaction will be sent to the test service, and if it contains a value of "false", the transaction will be sent to the live service. If this element does not exist, the default service will be utilised (usually the live service).</p> <p>Examples:</p> <pre><input type="HIDDEN" name="EPS_TEST" value="true"> <input type="HIDDEN" name="EPS_TEST" value="false"></pre>
EPS_3DSECURE [optional - ver 4+]	<p>This field may be set to either "true" or "false" and specifies whether the transaction contains extra 3D Secure parameters, supplied by Visa or Mastercard-compatible software.</p> <p>If 3D Secure processing is enabled, the following additional form parameters must be provided:</p> <p>3D_XID</p> <p>20-character Transaction ID string uniquely referencing this transaction to the merchant. This string must match the XID that was passed to the 3D Secure Merchant Plug-In at the password verification stage. The XID and CAVV will be checked by the accepting bank to ensure they match the verified transaction.</p> <p>May comprise of a timestamp padded with 0s for uniqueness, e.g.: "yyyyMMddHHmmsskkk000".</p> <p>3D_CAVV</p>

28-character Cardholder Authentication Verification Value string returned from the card issuer via the Merchant Plug-In at the password verification stage. Must be passed through exactly as it was returned from MPI.

3D_SLI

2-digit Security Level Indicator code returned from the card issuer to indicate whether the merchant is 3D Secure-enabled or not, and whether the XID and cardholder password were supplied and processed correctly. Must be passed through exactly as it was returned from MPI.

Examples:

```
<input type="HIDDEN" name="EPS_3DSECURE" value="true">
```

```
<input type="HIDDEN" name="3D_XID" value="20030306143821569000">
```

```
<input type="HIDDEN" name="3D_CAVV" value="7ftyhF5IMZE2ua60HQeCxc7IBaL">
```

```
<input type="HIDDEN" name="3D_SLI" value="05">
```

4 Parameter Formats

The format of a version 1 response is a text file, with HTTP content type of text/plain, containing four lines, separated by newline characters, in the following form:

- r = referenceID
- a = authorisationID
- m = message
- s = signature

The format of a version 2 response is a text file, with HTTP content type of text/plain, containing five lines, separated by newline characters, in the following form:

- r = referenceID
- a = authorisationID
- m = message
- s = signature
- e = eftResponse

The only difference between the version 1 and version 2 responses is the presence of the final field, the 'e' field, in the version 2 response. The format of a version 3 or 4 response is a similar text file, with HTTP content type of text/plain, containing seven lines separated by newline characters, this time with parameter names spelled out in full:

- ref-id = referenceID
- auth-id = authorisationID
- message = message
- signature = signature
- eft-response = eftResponse
- txn-id = bank transaction ID
- settlement-date = bank settlement date

4.1 Response Fields

These response fields are defined as follows:

Param ver 3+ in ()	Name	Description
R (ref-id)		The value from the EPS_REFERENCEID parameter of the request. If the merchant does not provide a reference ID, this field will contain an empty string. This value is returned to the merchant's processing system to allow matching of the original transaction request.
A (auth-id)		The transaction id as returned by the eSec Payment Gateway. This is an alphanumeric string that may be quoted by the merchant or the customer in future queries regarding the particular transaction. Using the HTTP Post Interface, this field <u>may</u> be set when the transaction was declined, therefore the "m" field should always be used to determine

Param Name ver 3+ in ()	Description
	success or failure of the transaction.
M (message)	<p>A response message from the Payment Gateway indicating the result of the transaction request. The message itself contains a number followed by a string describing the transaction result.</p> <p>All response messages follow the same general form: a three digit number followed by a space followed by a text message describing the result. The three digit numbers are broadly divided into three classes of responses: successful transactions (numbers within the 200-299 range); unsuccessful transactions (400-499 range); and Payment Gateway errors (numbers in the 500-599 range). Some messages may have a colon followed by varying text that further describes the error condition. For these messages, the text before the colon will always be constant.</p> <p>The possible messages that may be received by the merchant's processing system are:</p> <ul style="list-style-type: none"> • 200 success: The transaction has been processed and successfully authorised. Funds will be transferred to the merchant's bank account in an overnight banking settlement process • 400 refused: The transaction has been processed and authorisation was refused. Retrying the same transaction for the same credit card number is unlikely to be successful. • 401 invalid request: The transaction details provided are incorrect and the transaction cannot be processed. This is a fallback error response for unusual conditions and so while retrying the transaction with corrected data is possible, the Payment Gateway has been unable to provide exact details of the problem to assist the merchant's processing system. • 401 invalid merchant: XXXX The specified merchant identifier XXXX does not exist. Transactions that receive this response may be retried once the invalid data has been corrected. • 401 invalid reference id: The EPS_REFERENCEID parameter contains incorrect or invalid data. Transactions that receive this response may be retried once the invalid data has been corrected. • 401 invalid secParams: XXXX The EPS_SECPARAMS parameter XXXX is not a valid URL. Transactions that receive this response may be retried once the invalid data has been corrected. • 401 invalid amount: XXXX - The EPS_AMOUNT parameter XXXX contains either a non-numeric or non-decimal value. Transactions that receive this response may be retried once the invalid data has been corrected. • 401 invalid card type: XXXX - The EPS_CARDTYPE parameter XXXX contains a value that is not one of the possible values listed in the parameter description above. Transactions that receive this response may be retried once the invalid data has been corrected. • 401 invalid card number - The EPS_CARDNUMBER parameter contains a value that cannot be validated as a credit card number. The card number value is not included in the response message for security purposes. Transactions that receive this response may be retried once the invalid data has been corrected. • 401 invalid month: XX - The EPS_EXPIRYMONTH parameter XX does not contain an integer between the values of 1 through 12 inclusive. Transactions that receive this response may be retried once the invalid data has been corrected.

Param ver 3+ in ()	Name Description
	<ul style="list-style-type: none"> • 401 invalid year: XXXX - The EPS_EXPIRYYEAR parameter XXXX does not contain a value that can be determined to represent a year date. Transactions that receive this response may be retried once the invalid data has be corrected. • 401 invalid expiry: XX/XXXX - The specified expiry date, XX/XXXX, generated by combining the two EPS_EXPIRYMONTH and EPS_EXPIRYYEAR fields, does not represent a valid date in the future. Transactions that receive this response may be retried once the invalid data has be corrected. • 401 invalid name - The EPS_NAMEONCARD parameter incorrect or invalid data. The value of the EPS_NAMEONCARD parameter is not included in the response string for security purposes. Transactions that receive this response may be retried once the invalid data has be corrected. • 401 not SSL invocation - The SSL Web Interface CGI has been invoked using HTTP directly rather than via HTTP over SSL. Transactions that receive this response may be retried once the SSL invocation problem has been corrected. • 401 SSL key size too small - The length of the encryption key negotiated by the client system and the SSL Web Interface is too small to meet the minimum security level set for the merchant. Unless the merchant has requested a stronger level of security, the minimum key length is the normal 40 bit US-export grade SSL. Transactions that receive this response may be retried at a later time once the SSL invocation problem has been corrected. • 401 one http(s) resultURL required - The EPS_RESULTURL parameter does not contain a value. This parameter must contain a valid URL otherwise the Payment Gateway cannot proceed with the transaction. Transactions that receive this response may be retried at a later time once the EPS_RESULTURL parameter has a correct value. • 401 invalid resultURL parameter - The specified value of the EPS_RESULTURL parameter does not conform to the standard syntax for URLs. Transactions that receive this response may be retried at a later time once the resultURL parameter's value has been corrected. • 402 invalid response - An incorrect response has been received from the server and the transaction is considered to have not been processed. This response indicates a failure within the Payment Gateway itself and so the state of the transaction is not known. Retrying the transaction may be successful, however the merchant should contact technical support before doing so. • 500 internal failure - An internal problem has occurred and the transaction cannot be processed. This response indicates a failure within the Payment Gateway itself and so the state of the transaction is not known. Retrying the transaction may be successful, however the merchant should contact technical support before doing so. • 501 timeout - The transaction has taken too long and processing has been aborted. The Payment Gateway will take steps to try to reverse the transaction and it is considered to have not been processed. Transactions that receive this response may be retried at a later time. • 502 agent unavailable - A required service is unavailable and the transaction cannot be processed. This is a transient issue and transactions that receive this response may be retried at a later time. • 503 system unavailable - The server is unavailable, usually for scheduled maintenance, and the transaction cannot be processed. This is a transient issue and transactions that receive this response may be retried at a later time. <p>This parameter will always contain a message string from the list above. The merchant's</p>

Param Name ver 3+ in ()	Description
	processing system must be able to extract the number from the message to determine the result of the transaction. eSec reserves the right to add additional responses messages to this list without notification.
S (signature)	An encrypted signature of the transaction details. This is a base 64 encoded hexadecimal string that may be used to authenticate the transaction details, i.e. to verify that the transaction has been correctly processed by eSec and that nothing has been tampered with in transit. The signature may be verified with the CheckSig program that is provided as part of the Payment Gateway Real-time Shipping Enhancement. This argument will only be set if the transaction has been successfully processed and authorised (i.e. the response message in the 'm' parameter is "200 success").
E (eft-response) (ver 2+ only)	<p>The response code returned to the Payment Gateway by the financial institution that processed the transaction. This is an integer field with a valid range of 0 through 99 inclusive, and corresponds to the AS2805 response code from the EFT message. This field will only contain a value for 200 and 400 response codes. This field may contain one of the following values, although not all of these values will ever be returned by the Payment Gateway:</p> <ul style="list-style-type: none"> • 00 successful approval (corresponds to 200 response) • 01 refer to issuer • 02 refer to issuer's special conditions • 03 invalid merchant • 04 pickup card • 05 do not honour • 06 error • 07 pickup card, special conditions • 08 honour with ID (signature)(corresponds to 200 response) • 09 request in progress • 10 approved for partial amount • 11 approved VIP • 12 invalid transaction • 13 invalid amount • 14 invalid card number • 15 no such issuer • 16 approved, update track 3 • 17 customer cancellation • 18 customer dispute • 19 re-enter transaction • 20 invalid response • 21 no action taken • 22 suspected malfunction • 23 unacceptable transaction fee • 24 file date not supported • 25 unable to locate record on file

Param ver 3+ in ()	Name Description
	<ul style="list-style-type: none"> • 26 duplicate file update record, old record replaced • 27 file update field error • 28 file update file locked out • 29 file update not successful, contact acquirer • 30 format error • 31 bank not supported by switch • 32 completed partially • 33 expired card • 34 suspected fraud • 35 contact acquirer • 36 restricted card • 37 contact acquirer security • 38 allowable PIN retries exceeded • 39 no credit account • 40 request function not supported • 41 lost card • 42 no universal account • 43 stolen card • 44 no investment account • 45-50 reserved, will not be returned • 51 insufficient funds • 52 no cheque account • 53 no savings account • 54 expired card • 55 incorrect PIN • 56 no card record • 57 transaction not permitted to cardholder • 58 transaction not permitted to terminal • 59 suspected fraud • 60 contact acquirer • 61 exceeds withdrawal amount limit • 62 restricted card • 63 security violation • 64 original amount incorrect • 65 exceeds withdrawal frequency limit • 66 contact acquirer security • 67 hard capture • 68 response received too late • 69-74 reserved, will not be returned • 75 allowable number of PIN retries exceeded • 76-89 reserved, will not be returned

Param Name ver 3+ in ()	Description
	<ul style="list-style-type: none"> • 90 cutoff in progress • 91 issuer inoperative • 92 financial institution cannot be found • 93 transaction cannot be completed, violation of law • 94 duplicate transmission • 95 reconcile error • 96 system malfunction • 97 reconciliation totals have been reset • 98 MAC error • 99 reserved, will not be returned
(txn-id) (ver 3+ only)	<p>The bank transaction ID returned by the payment gateway. This 6-digit string is unique at least per terminal, per bank, per settlement day.</p> <p>The bank transaction ID can be used as a secondary reference for the transaction, after Transaction ID. This value is required to be re-entered along with other details of the original payment when conducting refunds through eSec's Merchant Login website.</p>
(settlement-date)](ver 3+ only)	<p>The bank settlement date returned by the payment gateway. This is the date the funds will be settled into the merchant's account. The date will correspond to today's date until the bank's cut-off time, then roll to the following business day.</p> <p>The settlement date is returned in the format "YYYYMMDD".</p>

It is possible to pass additional information to the result program by specifying such information as additional arguments to the primary result URL specified by the EPS_RESULTURL parameter. If the URL given by this parameter contains arguments, the Payment Gateway SSL Web Interface will simply append its own arguments to the end of the URL before invoking it.

Please note that this release of the Payment Gateway SSL Web Interface does not directly support the passing of other information through implied mechanisms such as cookies or session variables, although setting the EPS_REDIRECT parameter to a value of "true" may allow such mechanisms to function correctly. It is the responsibility of the merchant to ensure that chosen software products are compatible with the Payment Gateway.