



**eSec SSL Browser Redirect
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 SSL.....	4
2.1	Web Redirect Model.....	4
2.2	Web Proxy Model.....	5
3	The SSL Web Interface.....	7
4	Transaction Parameters	8

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 the eSec interface 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.

The Payment Gateway is also cost effective, providing merchants with the ability to authorise a credit card transaction for a flat handling charge only. The Payment Gateway brings e-commerce within reach of all merchants, regardless of their size.

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 SSL

The Payment Gateway SSL Web Interface may utilise either the [Web Redirect Model](#) or the [Web Proxy Model](#) for transaction management. The Web Proxy Model is used by default unless otherwise specified within the transaction parameters.

The Payment Gateway SSL Web Interface is intended to be driven via the use of an HTML form from within a web browser. While this interface may be integrated into an application-level environment, this usage is not recommended and the user is referred to the Payment Gateway Integration Interface for integration at this level.

This document is intended to be read and understood by web developers familiar with HTTP and HTML concepts. This is a technical document and does not attempt to explain web technologies.

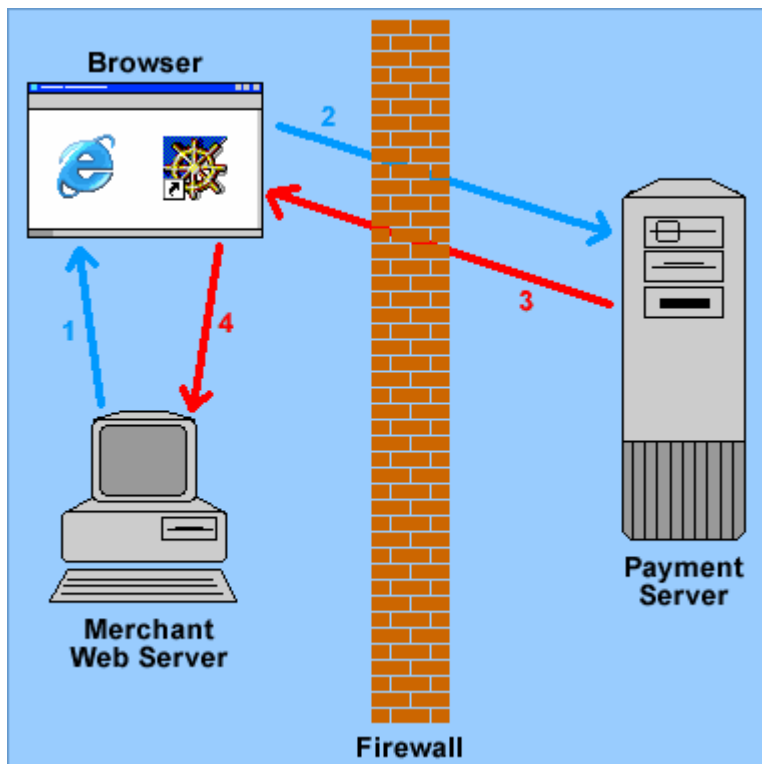


Throughout this document, sections which relate to Verified by Visa or MasterCard SecureCode implementation will be displayed like this, with the scheme logos to the left. These sections only relate to VbV and SecureCode merchants.

2.1 Web Redirect Model

The Web Redirect Model is a Web-specific interface for the Payment Gateway that can be integrated into a merchant Web site through the addition of some HTML code to a page on the Web site, and the provision of a response page or script to receive and process transaction results.

The Web Redirect Model is used by the [SSL Interface](#) product



The Web page containing the HTML code is sent to the client's browser from the merchant's Web site. When the client submits their purchase request, the browser transmits the request as a HTTP GET or POST request to the Payment Server and waits for a reply.

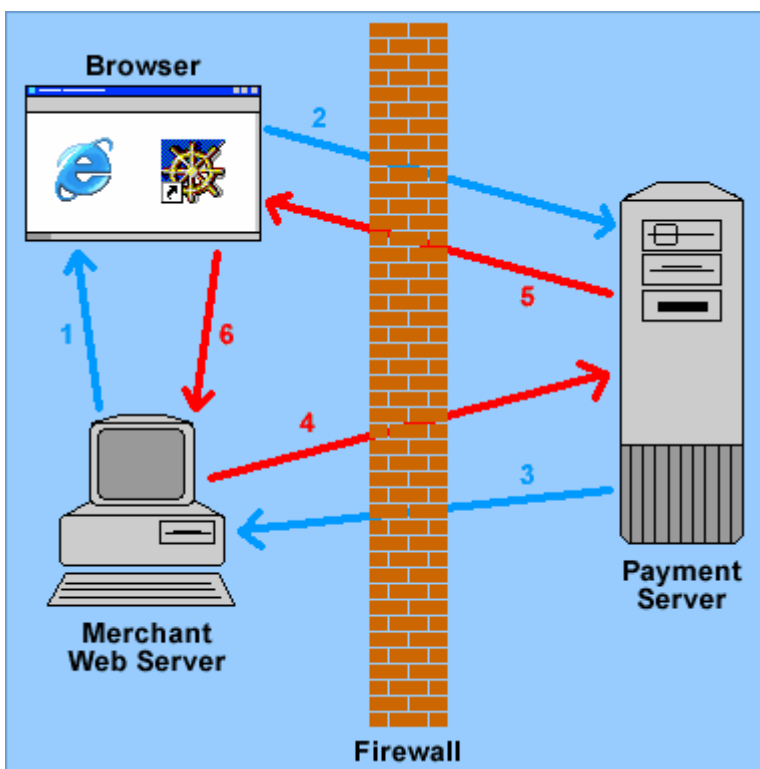
The transaction response is sent back to the browser as the result of the HTTP request. This response contains an instruction for the browser to redirect to the result page or script on the merchant's site, through the use of an HTTP "Location:" header, effectively relaying the result of the transaction back to the merchant's Web site.

This is the simplest interface model to implement from the merchant's point of view. It provides relatively fast performance and should interoperate with most 3rd party application environments, but has the lowest level of security of the supported interface methods since the browser is effectively an untrusted party in the transaction flow.

2.2 Web Proxy Model

The Web Proxy Model provides a higher level of security and more reliability than the Web Redirect Model, but is more susceptible to interoperability issues with 3rd party application environments. The integration requirements are identical to the Web Redirect Model, i.e. the addition of some HTML code to the merchant's Web site, and providing a response page or script to receive and process transaction results. Merchants may choose to switch between the Web Proxy Model and the Web Redirect Model with minimal change to their Web site.

The Proxy Model is used by the [SSL Interface](#) product



Like the Web Redirect Model, a Web page containing the HTML code is sent to the client's browser from the merchant's Web site. When the client submits their purchase request, the browser transmits the request as a HTTP GET or POST request to the Payment Server and waits for a reply.

The Payment Server sends the transaction response to the merchant's Web site by invoking the response page or script directly as a HTTP GET request, bypassing the client's browser. The Web page generated by the merchant's response page or script is then relayed to the client's browser as the transaction response page. This is an important point to note, as the page that will be displayed in the client's browser is generated by the merchant's Web site, not by the Payment Gateway.

This model is more complex than the Browser Indirect Model however it provides some significant advantages. The delivery of transaction results leaves footprints in Payment Gateway logs, allowing transaction issues to be easily traced. The transaction path is less reliant on the customer's browser, thus improving the overall reliability of the service and providing a better result delivery mechanism.

The primary disadvantage is an incompatibility with some 3rd party application environments that rely on cookies or other such mechanisms for passing session or state information. The Web Proxy Model is not supported for use with such application environments.

3 The SSL Web Interface

The parameters within the HTML form provide the information necessary for the Payment Gateway SSL Web Interface to determine how to process the requested transaction. These parameters, as noted below, must be provided by the merchant's processing system or gathered from the user. These parameters must be specified exactly as described in this document, 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:

LIVE:

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

TEST:

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

	<p>Verified by Visa and SecureCode merchants should use the URL: https://www.securepay.com.au/3dsecure/verifyEnrollment.jsp</p> <p>This URL handles the communication with card issuers and display of the password entry screen for the customer's card issuer, then redirects with appropriate authentication values to the payments page. The response to the merchant site will either be after the payment processing is complete, or if the customer's password entry is not authenticated by the issuer.</p>
---	--



4 Transaction Parameters

The Payment Gateway SSL Web Interface accepts transactional information as HTML form fields, transmitted using either a HTTP GET or POST method.

The transaction parameters are as follows:

<p>EPS_MERCHANT [required]</p>	<p>A 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="widgetrus"></pre>
<p>EPS_RESULTURL [required]</p>	<p>One or more parameters named EPS_RESULTURL must be passed to the Payment Gateway. One, and only one, of these parameters must contain the URL of a page on the merchant's web server that can accept and process CGI arguments. This parameter is referred to as the primary result URL, and the URL value it contains is known as the result page.</p> <p>The result page may be almost any form of web page, including static HTML pages, CGI scripts, ASP pages, JSP pages, PHP scripts, etc, however please note that cookies or other forms of additional information will not be passed through the Payment Gateway. The result page will be invoked by the Payment Gateway when the transaction has been processed and is used to pass the result of the transaction to the merchant's system.</p> <p>The primary result URL must be a URL for a publicly visible page on a web server within a domain that is delegated to a public IP number. Internal machine names, such as "localhost", Windows-style machine names, and privately translated IP numbers are not acceptable and will cause the Payment Gateway to fail.</p> <p>If more than one result URL parameter is given, all parameters after the first must contain only email addresses written as a URL, i.e. "mailto:myaddress@myserver.com.au". Each email address specified through a result URL parameter will be sent a standard form message each and every time a transaction is correctly processed by the Payment Gateway. Email messages will be sent for both successfully authorised and declined transactions.</p> <p>The following examples are provided to better illustrate the possible combinations of valid result URL parameter values.</p> <p>VALID: A primary result URL on its own EPS_RESULTURL=http://www.myserver.com.au/result.asp</p> <p>VALID: A primary result URL with a single mail address EPS_RESULTURL=http://www.myserver.com.au/result.asp EPS_RESULTURL=mailto:myaddress@myserver.com.au</p> <p>VALID: A primary result URL with multiple mail addresses</p>


	<p>EPS_RESULTURL=http://www.myserver.com.au/result.asp</p> <p>EPS_RESULTURL=mailto:myaddress@myserver.com.au</p> <p>EPS_RESULTURL=mailto:otheraddress@myserver.com.au</p> <p>EPS_RESULTURL=mailto:webmaster@myserver.com.au</p> <p>NOT VALID: A mail address on its own</p> <p>EPS_RESULTURL=mailto:myaddress@myserver.com.au</p> <p>NOT VALID: Two primary result URLs</p> <p>EPS_RESULTURL=http://www.myserver.com.au/result.asp</p> <p>EPS_RESULTURL="http://www.otherserver.com.au/cgi-bin/result.cgi"</p>
<p>EPS_REDIRECT [optional]</p>	<p>By default, the Payment Gateway SSL Web interface will utilise whichever transaction model has been configured for the merchant. The normal transaction model configured for merchants is the Web Proxy Model. The EPS_REDIRECT field may be used to explicitly set the transaction model for a transaction. This parameter, if specified, may contain either of the string values "true" or "false". If this parameter is set to "false", the proxy model will be used. If this parameter is set to "true", the Web Redirect Model will be used.</p> <p>Setting this field only affects the method by which the Payment Gateway invokes the URL specified as the primary result URL. The default behaviour will occur if the redirect field is not set, or if it contains an invalid value.</p> <p>If the merchant's processing system relies upon the passing of cookies for transmitting session information, the value of the redirect parameter should be set to "true". Cookies are not supported by the Payment Gateway Web SSL Interface when using the Web Proxy Model.</p> <p>Examples:</p> <pre><input type="HIDDEN" name="EPS_REDIRECT" value="true"> <input type="HIDDEN" name="EPS_REDIRECT" value="false"></pre>
<p>EPS_INFOEMAIL [optional]</p>	<p>An email address to which problem notifications should be sent. If a transaction problem occurs and the Payment Gateway is unable to notify the merchant's processing system through the normal method of invoking the primary result URL, an email message will be sent to the address specified by the infoemail parameter.</p> <p>This email address will only be used if either the primary result URL cannot be invoked, or if a network error is encountered while attempting to invoke it. If the merchant's primary result URL page generates any form of valid HTTP response, including error conditions, the merchant is considered to have been notified of the transaction and no email message will be sent.</p> <p>If no EPS_INFOEMAIL parameter is specified, the Payment Gateway does not notify the merchant of transaction errors</p> <p>Examples:</p> <pre><input type="HIDDEN" name="EPS_INFOEMAIL" value="mailto:me@domain.com"></pre>
<p>EPS_VERSION</p>	<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 is described later in this document. If not set to any value, the Payment Gateway assumes a</p>



	<p>Version 1 response.</p> <p>Examples:</p> <pre><input type="HIDDEN" name="EPS_VERSION" value="1"></pre> <pre><input type="HIDDEN" name="EPS_VERSION" value="2"></pre>  <p>Verified by Visa and SecureCode merchants <u>must</u> use version "4".</p>
<p>EPS_TEST [optional]</p>	<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"></pre> <pre><input type="HIDDEN" name="EPS_TEST" value="false"></pre>
<p>EPS_PASSWORD</p> 	<p>This is NOT the cardholder's password. The cardholder's Verified by Visa password or SecureCode should NEVER be collected by the merchant's website.</p> <p>This field is currently only required for Verified by Visa or SecureCode merchants. The field should contain the transaction processing password supplied by eSec when your Merchant ID is configured in our system.</p> <p>Example:</p> <pre><input type="HIDDEN" name="EPS_PASSWORD" value="password1"></pre>


The following parameters may be generated by the merchant processing system for each individual transaction. Many of these parameters will simply be named fields on an HTML form. Some of these parameters are optional and may be used to control certain aspects of the operation of the Payment Gateway.

The available parameters are:

<p>EPS_REFERENCEID [optional]</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>While the reference ID may be an optional parameter, it is highly recommended that the merchant's processing system utilise this parameter as an order number or invoice number to allow tracking of individual transactions.</p> <p>Examples:</p> <pre><INPUT TYPE="HIDDEN" NAME="EPS_REFERENCEID" VALUE="1234567890"></pre> <pre><INPUT TYPE="HIDDEN" NAME="EPS_REFERENCEID" VALUE="20010410-123456"></pre>
<p>EPS_CARDNUMBER [required]</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</p>

	<p>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 [required]</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> <pre><INPUT TYPE="HIDDEN" NAME="EPS_CARDTYPE" VALUE="testcard"> <INPUT TYPE="HIDDEN" NAME="EPS_CARDTYPE" VALUE="visa"></pre>
<p>EPS_EXPIRYMONTH [required]</p>	<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> <pre><INPUT TYPE="HIDDEN" NAME="EPS_EXPIRYMONTH" VALUE="1"> <INPUT TYPE="HIDDEN" NAME="EPS_EXPIRYMONTH" VALUE="12"></pre>
<p>EPS_EXPIRYYEAR [required]</p>	<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> <pre><input type="HIDDEN" name="EPS_EXPIRYYEAR" value="2008"> <input type="HIDDEN" name="EPS_EXPIRYYEAR" value="08"></pre> <p> Verified by Visa and SecureCode merchants <u>must</u> submit the expiry</p>

	<p>year as a 4-digit value, e.g. "2008", <u>NOT</u> "08".</p>
<p>EPS_CCV [mandatory for Verified by Visa and SecureCode merchants; otherwise optional]</p>	<p>The Card Check Value (CCV) field should contain the three digit value that is printed on the back of the credit card itself, or the four digit value printed on the front of American Express cards. 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, any 3 or 4 digit value will be accepted. 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> <p> Verified by Visa and SecureCode merchants <u>must</u> provide the CVV number for all payments, as a requirement of the schemes.</p>
<p>EPS_NAMEONCARD [required]</p>	<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> <pre><input type="HIDDEN" name="EPS_NAMEONCARD" value="John A. Citizen"> <input type="HIDDEN" name="EPS_NAMEONCARD" value="Jane M. Person"></pre>
<p>EPS_AMOUNT [required]</p>	<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> <pre><input type="HIDDEN" name="EPS_AMOUNT" value="10795"> <input type="HIDDEN" name="EPS_AMOUNT" value="107.95"></pre> <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 <u>with the trailing zeros intact</u>. If an amount such as AUD\$107.00 is simply submitted as 107, the Payment Gateway will assume that this is 107 cents 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 amount values will be rejected.</p> <p> Verified by Visa and SecureCode merchants <u>must</u> pass the amount <u>with</u> the decimal point in place. E.g. \$107.00 must be passed as "107.00".</p>

<p>EPS_3DSECURE [optional - ver 4+]</p> 	<p>Merchants <u>not</u> signed up for 3D Secure (Verified by Visa or SecureCode) should set this field to "false", or omit the field.</p> <p>Merchants using Verified by Visa or SecureCode, or both, must set this field to "true"</p> <p>If 3D Secure processing is enabled, the following additional form parameters must be provided:</p> <p>3D_XID</p> <p>3D Secure Transaction ID string. MUST uniquely reference this transaction to the merchant, and MUST be 20 characters in length. Any ASCII characters may be used to build this string.</p> <p>E.g. May comprise of a timestamp padded with 0s for uniqueness: "20040714112034872000".</p> <p>MerchantID</p> <p>Your online merchant number specified by your <u>acquiring bank</u> which has been registered for Verified by Visa or SecureCode, or both. For Westpac customers this should be your 8 digit merchant number, e.g. "22123456".</p> <p>Examples:</p> <pre><input type="HIDDEN" name="EPS_3DSECURE" value="true"> <input type="HIDDEN" name="3D_XID" value="20040714112034872000"> <input type="HIDDEN" name="MerchantID" value="22123456"></pre>
--	---

Once the Payment Gateway SSL Web Interface has completed the processing for a transaction, it will notify the merchant's processing system of the transaction's outcome by invoking the result page as specified by the primary result URL.

Occasionally the Payment Gateway may choose to generate an error page for the user if the transactional information provided is deemed to be unacceptable. This occurs most commonly when a null or incorrect value has been specified for the primary result URL, and is part of the normal operation of the service.

The result page specified by the primary result URL is passed a set of parameters using the CGI conventions. Most web server and application environments will automatically translate these parameters into a more useful form, so please check the documentation for your web server or application environment for more information. Given the large number of web-based products available, eSec support staff will not necessarily be able to assist you with issues specific to your chosen software product.


For a Version 1 response, there are four CGI parameters passed to the merchant's primary result URL page using an HTTP GET method. These parameters are named 'r', 'a', 'm' and 's'.

For a Version 2 response, there are five CGI parameters passed to the merchant's primary result URL page, also using an HTTP GET method. This response form includes the same four parameters from the Version 1 response, i.e. the 'r', 'a', 'm' and 's' parameters, and add a fifth parameter named 'e'.

For a Version 3 or 4 response, there are seven CGI parameters passed to the merchant's primary result URL page, also using an HTTP GET method. The response form includes the same five parameters from the Version 2 response, and a 6th and 7th parameter. Parameter names are spelled out in these versions, i.e. 'ref-id', 'auth-id', 'message', 'signature', 'eft-response', and new parameters, 'txn-id', and 'settlement-date'.

Param Name <small>ver 3+ in ()</small>	Description

Param Name ver 3+ in ()	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 of between 1 and 6 characters that may be quoted by the merchant or the customer in future queries regarding the particular transaction. Using the SSL Interface, this field <u>may</u> be set when the transaction was declined, therefore the "m" field should always be used to determine 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

Param Name <small>ver 3+ in ()</small>	Description
	<p>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.</p> <ul style="list-style-type: none"> • 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. • 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 been 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 been 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 been 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. •  401 Cardholder authentication failed - The cardholder password entered for Verified by Visa or SecureCode failed and the financial transaction has not been processed by the bank. • 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.

Param Name <small>ver 3+ in ()</small>	Description
	<ul style="list-style-type: none"> • 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 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.</p>
S (signature)	<p>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").</p>
E (eft-response) <small>(ver 2+ only)</small>	<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

Param Name <small>ver 3+ in ()</small>	Description
	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
	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

Param Name <small>ver 3+ in ()</small>	Description
	<p>55 incorrect PIN</p> <p>56 no card record</p> <p>7 transaction not permitted to cardholder</p> <p>58 transaction not permitted to terminal</p> <p>59 suspected fraud</p> <p>60 contact acquirer</p> <p>61 exceeds withdrawal amount limit</p> <p>62 restricted card</p> <p>63 security violation</p> <p>64 original amount incorrect</p> <p>65 exceeds withdrawal frequency limit</p> <p>66 contact acquirer security</p> <p>67 hard capture</p> <p>68 response received too late</p> <p>69-74 reserved, will not be returned</p> <p>75 allowable number of PIN retries exceeded</p> <p>76-89 reserved, will not be returned</p> <p>90 cutoff in progress</p> <p>91 issuer inoperative</p> <p>92 financial institution cannot be found</p> <p>93 transaction cannot be completed, violation of law</p> <p>94 duplicate transmission</p> <p>95 reconcile error</p> <p>96 system malfunction</p> <p>97 reconciliation totals have been reset</p> <p>98 MAC error</p> <p>99 reserved, will not be returned</p>
(txn-id) <small>(ver 3+ only)</small>	<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) <small>(ver 3+ only)</small>	<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, and 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.