e Merchant Plug-in (MPI) Integration & User Guide

Enabling merchants to integrate their payment processing with SECPay's 3-D Secure Merchant Plug In (MPI) solution.

This document provides the details of the 3-D Secure protocol, SECPay MPI and integration into the various payment gateways on offer.

Related services such as transaction reporting and test simulator operating procedures are also covered.

CONTENTS

1. Inclusions

SECPay's 3-D Secure counter-fraud solution (Verified by Visa and MasterCard SecureCode) is offered to SECPay merchants that have the following acquiring banks :

- HSBC
- Barclays Merchant Services (BMS)
- Streamline (NatWest)
- Bank of Scotland (BOS)
- Lloyds TSB
- EuroConex
- Alliance and Leicester

.
JCB J-Secure will be available in the near future, offering similar functionality to the Visa and MasterCard 3-D Secure protocol.

To ensure that you have the most current version of this document, please visit www.secpay.com and click on integration guides from the home page.

SECPay offers merchants a wide range of payment gateways to process transactions, including SECCard/SECPage (ValCard) service, XMLValCard XML-RPC, SOAP and VPN payment gateways.

2. Exclusions

This service cannot be used in conjunction with SECBatch or Mail Order/Telephone Order (MOTO) transactions including SECTerminal as the service requires the card holder to authenticate the transaction in real-time, accordingly batch and MOTO processed transactions cannot be authenticated in this way.

- Paymentech Salem
- Paymentech Tampa

Currently there are limitations on 3-D Secure authentication on UK issued Switch, Switch/Maestro and Maestro as well as UK issued SOLO cards. Please see section 3.7.

3. Introduction to 3-D Secure

In general, internet based credit and debit card transactions have been classified as 'cardholder-not-present' (CNP) and 'no signatory present'.

Historically, merchants have been vulnerable to instances where the on-line shoppers have denied the validity of the transaction. In such disputed cases (which are typical for on-line fraud cases) if merchants' where unable to prove that the actual cardholder was the person performing the payment transaction on their website, the merchant would have to bear the total cost, including the chargeback costs from the acquiring bank. Integrating the 3-D Secure technology on the merchant's website shopping system allows them to verify and authenticate the true identity of the shopper in real-time, thereby dramatically reducing their exposure to disputed transactions of this type.

3-D Secure is a credit card authentication program implemented by Visa and MasterCard to reduce fraudulent purchases by verifying purchaser identity during online transactions.

The benefits of implementing 3-D Secure include a reduction in disputed transactions and chargebacks and their resulting financial expense. Visa has branded this as 'Verified By Visa', and MasterCard has branded their equivalent as MasterCard SecureCode. Both of these protocols are brand identities for the 3-D Secure cardholder authentication scheme.

3-D Secure is a payments protocol based on an architecture known as the "Three Domain Model" (figure 3.1) and builds on proven SSL technology to provide a standard, secure method of performing transactions over the Internet through authentication of all parties involved in an online transaction.

The three domains are:

1. Issuer Domain
The issuer is responsible for managing the Enrolment of their cardholders in the service and the authentication of the cardholder during an online purchase.

2. Acquirer Domain
The acquirer is responsible for ensuring that the merchant participating in the transaction are operating under a merchant agreement and also for the actual processing for the authenticated transaction.

3. Interoperability Domain

This domain facilitates the transaction exchange between the other two domains with a common protocol and shared services.

Fig. 3.1 : 3-D Secure Three Domain Model

For more information about Verified By Visa Secure read the Visa 3-D Secure Introduction Information or visit the Visa 3-D Secure homepage.
Additional links and information about MasterCard SecureCode can be found at the MasterCard SecureCode FAQ or the MasterCard SecureCode homepage.

3.1. How Does 3-D Secure Work?

MasterCard® SecureCode™ and Verified By Visa (VBV) run from the merchant's or Payment Service provider's website and interacts with both the customer and their card issuer. When your customer is confirming the payment for the transaction, a simple pop-up box or in-line window appears asking them to enter a private code that has been registered with their bank. It passes the authentication value in your normal authorisation request procedures and, if approved, receives an authorisation that binds that customer to that transaction. This authentication value is transported using a Visa or MasterCard® data field. The customer's bank then validates that code and provides the merchant with a means of achieving a fully verified transaction.

3.2. Enrolment and Authentication

3-D Secure mechanism comprises of two main functions; Enrolment and Authentication.

3.2.1. Enrolment:

Enrolment is the process by which cardholders are enabled to use the 3-D Secure Services. When cardholders enrol, they are asked for relevant identification information as well as personal information such as a password and a Personal Assurance Message. Once this data is collected and the Issuer has verified the cardholder's response, he is considered to be 'enrolled', in 3-D Secure methodology. The Enrolment Server tracks participating cardholders and passes the record of Enrolment to the Issuer's Access Control Server (ACS). Each time the cardholder conducts a transaction for which a 3-D secure authentication request is generated; this ACS will be queried, to certify that the cardholder is in fact enrolled in 3-D Secure.

A typical enrolment process would constitute the following steps:

1. Cardholder goes to Issuer enrolment web pages, providing card details and other identification information specified by the Issuer along with any other required shared secret information, such as a password or Personal Assurance Message.

2. Issuer Validates Cardholder information and notifies the cardholder of successful completion of the enrolment process.

3. Enrolment Server supplies an update to the Access Control Server (ACS), including the newly enrolled card number and any other data required for subsequent purchase authentication; such as a password, PIN, etc.

3.2.2. Authentication

On enrolment, the cardholder is ready to shop at any participating merchant site where the merchant is 3-D Secure enabled. Merchants are 3-D Secure enabled by integrating their site with the 3-D Secure Merchant Plug-In (MPI), which can be obtained by the merchant from a Payment Service Provider (PSP) such as SECPay.

The Merchant Server Plug-in (MPI) obtains the cardholder information and is able to access the Visa or SecureCode Directory Server (DS) to validate the cards participation in the service.

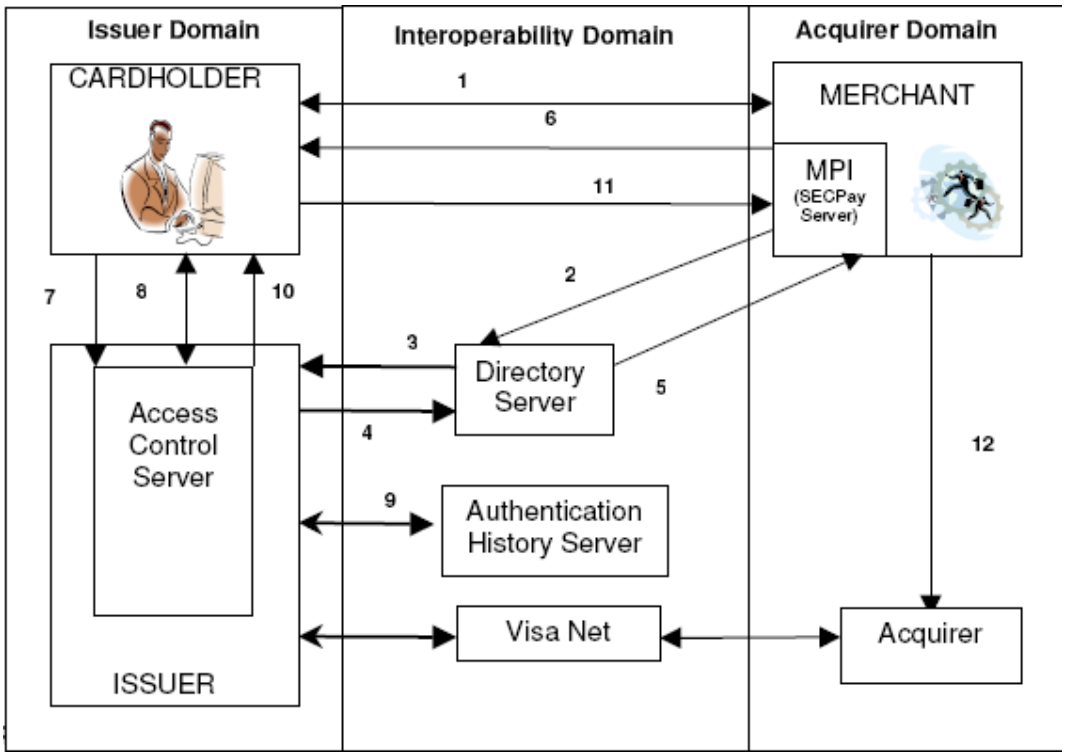
After the cardholder clicks “Buy” or “Check-out”, the MPI (SECPay) sends a message to the Directory Server containing the cardholder account number. Through an exchange of messages, the Visa Directory and the issuer’s Access Control Server (ACS) determine if the cardholder is enrolled in 3-D Secure. A message is returned to the Merchant Server plug-in, indicating the result. The MPI then sends an authentication request to the ACS through the cardholder’s browser and the ACS performs the authentication routine defined by the Issuer; e.g., it may display a password entry or display the PIN entry, etc., as the case may be. This varies between Issuers and the Visa-3D model offers the flexibility for each issuer to choose its authentication routine. The ACS now sends the results of the authentication to the Merchant Server Plug-in. If this response from the ACS indicates successful authentication, the MPI returns the successful authentication response to the Merchant and the transaction is processed as usual.

A Sample Authentication Process can be summarized as follows (Please refer the table in figure -3.2(a) and the diagram shown in figure of 3.2(b)) :

3-D Secure Transaction Message Flow Description

STEP	DESCRIPTION
1	Shopper browses at merchant site, adds items to shopping cart, then finalises purchase. (Note: Merchant now has all necessary data, including Personal Account Number (PAN) and user device information.)
2	Merchant Server Plug-in (MPI) sends PAN (and user device information, if applicable) to Directory Server.
3	Directory Server queries appropriate Access Control Server (ACS) to determine whether authentication (or proof of authentication attempt) is available for the PAN and device type. (If no appropriate ACS is available, the Directory Server creates a response for the MPI and Processing continues with Step 5.)
4	ACS responds to Directory Server.
5	Directory Server forwards ACS response (or its own) to MPI. If either authentication or proof of authentication attempt is NOT available, 3-D Secure processing ends, and the merchant, acquirer, or payment processor may submit a traditional authorisation request, if appropriate.
6	MPI sends Payer Authentication Request to ACS via shopper's device.
7	ACS receives Payer Authentication Request.
8	ACS authenticates shopper using processes applicable to PAN (Password, chip, PIN, etc.). Alternatively, ACS may produce a proof of Authentication Attempt. ACS then formats Payer Authentication Response message with appropriate values and signs the message.
9	ACS sends Authentication data to Authentication History Server.
10	ACS returns Payer Authentication Response to MPI via shopper's web browser. ACS sends selected data to Authentication History Server.
11	MPI receives Payer Authentication Response. MPI validates Payer Authentication Response signature.
12	Merchant proceeds with authorisation exchange with its acquirer.
	Following Step 12, acquirer processes authorisation with issuer via an authorisation system such as Visa Net and returns the results to merchant.

Fig. 3.2(b): 3-D Secure Transaction Message Flow



Without the 3-D Secure technology Internet merchants are vulnerable to lost revenues and costs associated with charge backs, and fines. Merchants that interface their credit card clearing process to the 3-D Secure merchant plug-in interface (MPI) technology are protected against most instances of fraud-related charge backs. Customers can shop more safely and merchants can avoid charge backs resulting from "I didn't do it" claims. Both VISA and MasterCard® have implemented chargeback liability shift policy for these "I didn't do it" chargebacks when the transaction is authenticated through Verified By VISA or MasterCard® SecureCode™.

3.4. 3-D Secure – Merchant Benefits

The primary benefit of 3-D Secure is the shift of liability from the merchant to the issuer/cardholder on **certain types** of disputed online credit card transactions. This liability factor has been the cause of major concern to most online vendors and service providers. In a standard online credit card transaction, when the cardholder or issuer disputes a transaction (as being fraudulent), then the merchant is liable to pay back the disputed charges. For example, a cardholder purchases a product or a service online from a merchant and upon receiving the goods/service, goes to his card issuer and claims the transaction as fraudulent. In this case, the merchant is liable to refund the disputed amount to the cardholder. With 3-D Secure this liability shifts to the card issuer.

3.5. 3-D Secure – Cardholder Benefits

For the cardholder, 3-D Secure provides increased confidence that your card details are secure when purchasing over the internet.

3.6. The business case for Internet merchants using SECPay

- 70% of e-commerce chargebacks are "cardholder unauthorised" due to cardholders saying, "I didn't do it." SECPay gives you a way to reduce chargeback and fraud costs.
- 70% of consumers surveyed by MasterCard® say they are concerned with security and fraud issues. SECPay gives them more confidence.
- 73% say that enhanced security would influence their decision to purchase online. SecureCode™ encourages online shopping.
- 61% are concerned that their credit card number will be intercepted by "hackers".
- Accepting cards from other countries will be easier and less risky; SECPay helps you move into new markets.
- Free advertisement on Visa and MasterCard®'s consumer websites.

Note: the above information is based on data published on the MasterCard®'s website.

3.7. Card Types Supported by 3-D Secure

The following card types for each scheme are supported for 3-D Secure authentication * :

VISA: Verified By Visa

- Visa Credit
- Visa Debit
- Visa Commercial (European Issued Cards ONLY)
- Visa Electron

MASTERCARD: SecureCode

- MasterCard Credit (including Business cards)
- International Maestro (Internationally Issued ONLY)
- UK Domestic Maestro (also known as Switch or Switch/Maestro)
    - Supported by the following Acquiring Banks ONLY:
        1. EuroConex
        2. Alliance & Leicester
        3. Lloyds TSB
        4. Bank of Scotland (BOS)
        5. Streamline (NatWest)
        6. HSBC
- Solo

- Supported by the following Acquiring Banks ONLY:
  1. EuroConex
  2. Alliance & Leicester
  3. Lloyds TSB
  4. Bank of Scotland (BOS)
  5. Streamline (NatWest)
  6. HSBC

*** NOTE*: Due to the complexity of differing policies and procedures as well as the frequency of change amongst the acquiring banks SECPay cannot accept responsibility for any incorrect information regarding Liability Shift in this document. MERCHANTS MUST refer to their acquirer documentation for more information on liability shift or the Visa/MasterCard Merchant Implementation Guides. Please refer to section 3.8 (below) for an overview of the operating principles behind liability shift.***

3.8. Levels of Liability Shift Protection and Implementation Guides

The level of liability shift can differ, depending on where the card was issued, the type of authentication gained. The following provides a summary of liability shift *:

VISA

- Full global cover (Visa Intra and Inter Regional) for fully authenticated and successfully attempted authentication (Note: Visa rules differ for Commercial cards)

MASTERCARD

- Cover as per following table ('*' = merchant only liability shift) :

Acquiring Region	US	CAN	EUR	LA/C	AP	SAMEA
US	Fully authenticated liability shift only	*	*	*	*	*
CAN	*	Fully authenticated liability shift only	*	*	*	*
EUR	*	*	*	*	*	*
LA/C	*	*	*	*	*	*
AP	*	*	*	*	*	*
SAMEA	*	*	*	*	*	*

- EU Merchants - Verified by Visa Merchant Implementation Guide
  http://www.visaeurope.com/documents/vbv/verifiedbyvisa_3dsecure.pdf
  Verified by Visa and CVV2
  http://www.visaeurope.com/documents/vbv/verifiedbyvisa_cvv2.pdf
- USA Merchants - Verified by Visa Merchant Implementation Guide
  https://usa.visa.com/cpf/business/accepting_visa/verified_mig_form.jsp
- MasterCard SecureCode Merchant Implementation Guide
  http://www.mastercardmerchant.com/securecode/getstarted.html

Barclays Merchant Services (BMS) have produced their own Merchant Implementation Guide which covers both Visa VBV and MasterCard SecureCode. The Implementation Guide can be found at the following URL link:

- BMS 3-D Secure Merchant Implementation Guide
  http://www.epdq.com/docs/BCD01122-IAPG-Auth.pdf

3.9. Verified by Visa and MasterCard SecureCode Logos

Merchants must display the Verified by Visa and SecureCode Merchant mark while certified 3-D Secure software is in operation. The logos will allow your customers to visibly see that you are participating in each of the schemes.

The Verified by Visa and SecureCode Merchant mark must be displayed on the checkout page and it is recommended that the mark should be displayed on the home page and /or security information page.

If a merchant is using SECPay's standard template which is hosted on our server, the logos will automatically appear when the merchant has been enabled on SECPay's server. Other merchants can us the following tag in their customised template, only if the template is hosted on our server:

${3ds}

alternatively the whole link can be used as follows:

- **Visa**

<ahref="http://www.visa.com/verified" target=_blank><img border="0" src="https://www.secpay.com/images/vbv.gif" ALT='Verified by Visa'>

- **MasterCard**

<A href= "http://www.mastercardbusiness.com/mcbiz/index.jsp?template=/orphans&content=securecodepopup"><IMG SRC="https://www.secpay.com/images/sc.gif" BORDER=0 ALT='MasterCard SecureCode' target=_blank></A>).

The logos should only be displayed while the merchant is participating in the scheme.

4. SECPAY'S 3-D Secure MPI SOLUTION AND INTEGRATION

SECPay have developed their own MPI which is listed on both the Visa and MasterCard websites:

- Visa Vendor List
- MasterCard Vendor List

SECPay's payment gateways have been updated to support 3-D secure transactions. The additional functionality required to perform a 3D authentication is included within our MPI.

4.1 SECCard/SECPage (ValCard) Gateway Integration

Our on-line merchants interface their systems with SECPay's hosted MPI by adding a link to a secured URL. Please refer to the SECCard Integration guide for more information on general integration information and parameters required. For current SECCard/SECPage merchants, the integration is almost seamless and the only requirement is to register for participation in the service and ask for the service to be activated at SECPay. The merchant will be required to display logos similar to those shown, on their website and pass extra parameters to the payment gateway as listed in the table of figure 4.1. Please refer to section 3.9 for more information on displaying the logos.

Fig. 4.1: 3-D Secure Extra Parameters

Parameter	Description	Length	Inclusion
mpi_description	Order Description. A brief description of items purchased.	0 – 125 characters	Optional. It is advisable to include this field in case of disputes.
mpi_merchant_name	Merchant Name to be displayed on the authentication page	1 – 25 characters	Required if not using value on SECPay database
mpi_merchant_url	Fully qualified URL of Merchant website	1 – 2048 characters	Required if not using value on SECPay database

The format of the parameters of figure 4.1 are as follows:

<input type="hidden" name="mpi_description" value="Widgets">

<input type=”hidden” name=”mpi_merchant_url” value=”http://www.yourserver.com/”>
<input type=”hidden” name=”mpi_merchant_name” value=”Merchant Name”>

From here on, SECPay manage the entire authentication process. SECPay initiates, coordinates and engages in the authentication and validation processes between all parties including the acquirer, the issuer Visa and MasterCard®. When the process is complete, the session will be redirected back to your gateway.

4.1.1. SECCard 3-D Secure Transaction Flow

The diagram of figure 4.2(a) shows a sample 3D Authentication process for merchants utilising the SECCard payment gateway. The table of figure 4.2(b) summarises the cardholder authentication process for those merchants using the SECCard payment gateway.

Fig. 4.2(a): 3-D Secure SECCard Authentication Message Flow

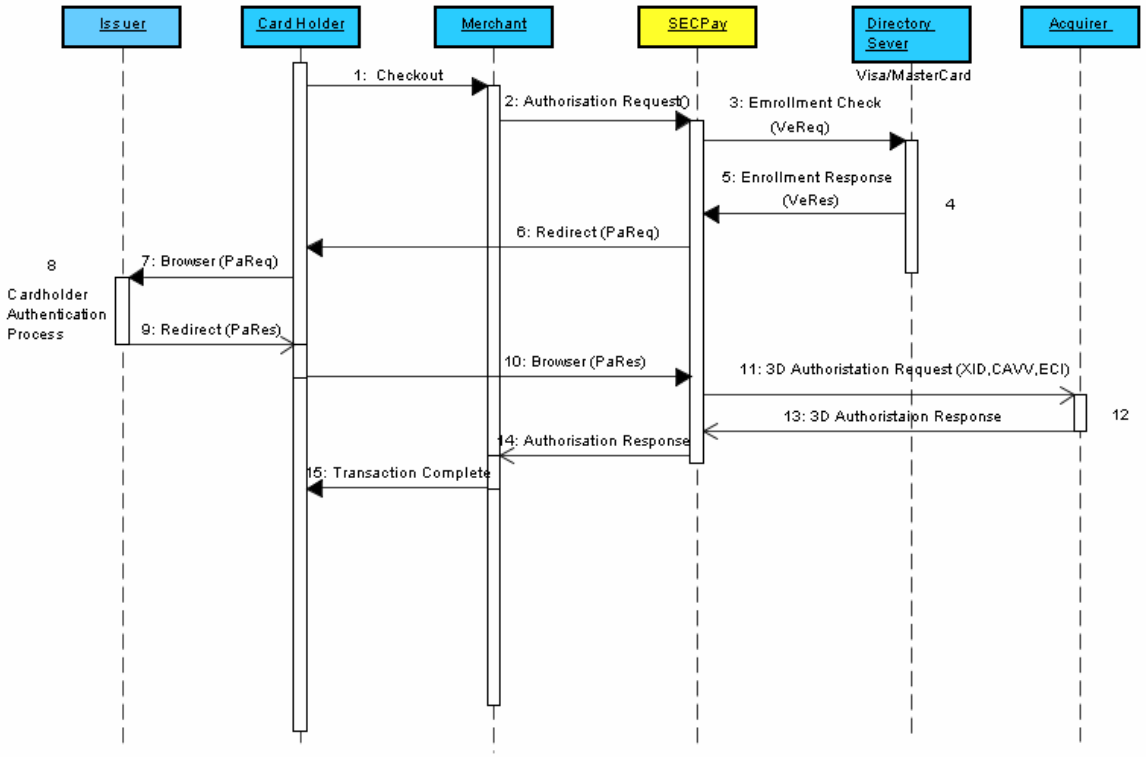


Fig. 4.2(b) : 3-D Secure Transaction Message Flow Description

STEP	DESCRIPTION
1	Shopper browses at merchant site, adds items to shopping cart, then finalises purchase.
2	The merchant payment page is populated with all the necessary details (Note: Merchant now has all necessary data, including PAN and user device information.) and an authorisation request is sent to SECPay's SECCard payment gateway (ValCard).
3	SECPay's Merchant Server Plug-in (MPI) sends a Verify Enrolment Request (VEReq) to the Directory Server.
4	• Directory Server queries appropriate Access Control Server (ACS) to determine whether authentication (or proof of authentication attempt) is available for the PAN and device type. • ACS responds to Directory Server (If no appropriate ACS is available, the Directory Server creates a response for the MPI and Processing continues with Step 5.)
5	Directory Server forwards Verify Enrolment Response (VERes) ACS response (or its own) to SECPay's MPI. SECPay MPI validates the VERes
6/7	MPI sends Payer Authentication Request (PAReq) to ACS via shopper's web browser.
8	• ACS receives Payer Authentication Request. • ACS authenticates shopper using processes applicable to PAN (Password, chip, PIN, etc.). Alternatively, ACS may produce a proof of Authentication Attempt. • ACS then formats Payer Authentication Response message with appropriate values and signs it.
9/10	• ACS returns Payer Authentication Response to MPI via shopper's Web browser. ACS sends selected data to Authentication History Server. • MPI receives Payer Authentication Response. • MPI validates Payer Authentication Response signature.
11	SECPay sends 3D Authorisation Request to the acquiring Bank. This includes the addition of XID, CAVV and ECI values.
12	Acquirer processes authorisation with issuer via an authorisation system such as Visa Net and returns the results to SECPAY.
13/14/15	SECPay receives 3D Authorisation Response from the acquirer and forwards the result to the merchant

4.2. SECPay XMLValCard Gateway Integration

SECPay merchants' interface their systems with SECPay hosted MPI by adding a link to a secured URL. Refer to the SECCard Integration guide for more information on general integration information and parameters required.

As part of 3-D Secure, merchants' are required to display logos, similar to those shown below. Please refer to section 3.9 for more information on displaying the logos.

The next two sections describe the steps involved to allow the merchant to successfully integrate XMLValCard to perform 3-D Secure authentication.

4.2.1. Enrolment Request

For a 3-D Secure transaction, the merchant's customer enters their details into the merchant's payment page as for a non 3-D Secure transaction. The merchant's website then makes a secure SSL call to SECPay's XMLValCard payment gateway as with a normal payment gateway call. However, with a 3-D Secure transaction, the process is significantly different. The merchant must supply all the mandatory parameters to allow SECPay's MPI to check the enrolment status of the card and, if necessary, generate a PAReq message that is required by the card issuer. The way in which the merchant's software gathers this extra data is not within the scope of this document and it is assumed that your web application can capture and/or generate the required data.

The extra parameters are shown in figure. 4.3, which are required to perform a 3-D Secure Enrolment request. The data is required to build a PAReq if the cardholder is enrolled for 3-D Secure.

A typical XML Request for a 3-D Secure transaction is shown in figure 4.4

Fig 4.3: D-Secure enrolment extra request parameters

URL CALL: https://www.secpay.com/java-bin/XMLValCard

PARAMETER	EXAMPLE	DEFINITION
device_category	0	Indicates the type of device or channel being used for shopping. A value of 0 (zero) indicates a standard web browser; a value of 1 (one) indicates a mobile WAP based browser. Optional – If omitted a value of 0 is implied.
accept_headers	image/gif, image/ x-xbitmap, image/jpeg, image/pjpeg, application/ vnd.ms-excel, application/ vnd.ms-powerpoint, application /msword, application/ x-shockwave-flash, */*	The exact content of the HTTP accept header as sent to the merchant from the cardholder's user agent. Determined from the web server environment. Required if the cardholder's user agent supplied a value.
user_agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)	The exact content of the HTTP user-agent header as sent to the merchant from the cardholder's user agent. Determined from the web server environment. Required if the cardholder's user agent supplied a value.
mpi_merchant_name	Your Company Name	Merchant Name to be displayed on the authentication page (0 – 125 characters). Required if not using value on SECPay database.
mpi_merchant_url	http://yoururl.com	Fully qualified URL of Merchant website (0 – 2048 characters. Required if not using value on SECPay database
mpi_description	Widgets	Order Description. A brief description of items purchased (0 – 125 characters). Optional. It is advisable to include this field in case of disputes.
purchaseRecurringFrequency	1	Required if the merchant and cardholder have agreed to recurring payments. The minimum number of days between authorizations (0-4 digits)

PARAMETER	EXAMPLE	DEFINITION
purchaseRecurringExpiry	20041210	Required if the merchant and cardholder have agreed to recurring payments. Date after which no authorizations should be performed (YYYYMMDD)
purchaseInstallments	2	Maximum number of permitted authorizations for installment payments (0 - 3 digits)

Fig 4.4: 3-D Secure enrolment extra request parameters

```
<XMLRequest>
        <merchant>secpay</merchant>
        <trans_id>xmltest</trans_id>
        <amount>10.50</amount>
        <options>dups=false</options>
        <card_no>4012001037141112</card_no>
        <expiry>0106</expiry>
        <customer>Fred Bloggs</customer>
        <ip>192.168.4.25</ip>
        <device_category>0</device_category>
        <accept_headers>image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword,
application/x-shockwave-flash, */*</accept_headers>
        <user_agent>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR
1.0.3705)</user_agent>
</XMLRequest>
```

SECPay's payment gateways will respond with the results of the enrolment check; Figure 4.5 shows a sample response. The **mpi_status_code** field indicates what action should be taken next.

Fig 4.5: 3-D Secure Enrolment Response

```
XMLResponse>
        <valid>true</valid>
        <trans_id>xmltest</trans_id>
        <test_status>true</test_status>
        <hash>3503eeb333701f6cb4b38556e6c3e7e3</hash>
        <mpi_status_code>212</mpi_status_code>
        <mpi_message>Cardholder Not Participating</mpi_message>
</XMLResponse>
```

In general, after the enrolment request response is received and if the merchant receives one of the status codes as shown in figure 4.5, the liability shift offered by 3-D Secure can be obtained or in the case of a MPI status code of 200, the cardholder has to be redirected to the card issuer and authenticated to gain liability shift. Any other code indicates that liability shift was not obtained or an error occurred in which case no liability shift was obtained. Please refer to section 3.8 for more information on liability shift. Please refer to Appendix A for the possible status codes that can be returned by the MPI.

Fig. 4.6: 3-D Secure Payer Verification Required Status Code

MPI Status Code	Description	Action
200	Payer Verification Required	The payer should now be redirected to the issuer to be authenticated.
212	Cardholder Not Enrolled	The cardholder is not enrolled for 3-D Secure

NOTE: The merchant's software should be designed to accommodate future enhancements to SECPay's MPI and allow for additional MPI return codes as and when they are added by the acquiring banks as well as SECPay.

In the case of all MPI status codes except code 200, SECPay will attempt to authorise the transaction with the acquiring bank, and the result will be returned to the merchant in the format as shown in figure 4.4

The only extra parameters returned by the XMLValCard gateways are:

mpi_status_code (Refer to Appendix A)
mpi_message (user-friendly description of the status code)

4.2.2. 3-D Secure Cardholder Authentication Process

Before 3-D Secure, SECPay returned the result of the authorisation attempt from the merchant's acquiring bank and the merchant displayed the result to the cardholder. However, with the 3-D Secure scheme and if a status code of 200 is returned from SECPay's MPI, the cardholder is required to be authenticated. To enable the cardholder to be authenticated, the cardholder must be redirected to the card issuer via a redirect page. This section shows you how to construct the basic page.

The information that is added to the page are 3 fields returned by the MPI and 1 field added by the merchant's server as shown in figure 4.7:

Fig. 4.7: MPI return parameters

Parameter	Description
acs_url*	The URL of the issuers Access Control Server which the cardholder is redirected to
MD*	Unique reference used by all parties including SECPay and the merchant to identify and track the 3-D Secure transaction
PaReq*	The Payment Authentication Request that the card issuer users for the authentication process
TermUrl	TermUrl contains the URL on the merchant's server where the cardholder is redirected to following authentication by the issuer's ACS.

**** These fields are extracted from the SECPay XMLValCard 3-D Secure enrolment response.***

When all the necessary data is extracted from the enrolment check response, the merchant's application is required to construct and return a page similar to the one in figure 4.8, which redirects the cardholder's browser to the issuer's ACS. The TermUrl contains the URL on the merchant's server where the cardholder is redirected to following authentication by the issuer's ACS.

Fig. 4.8 : 3-D Secure Redirect Page

```
<html>
<head>
<title> 3-D Secure Verification</title>
</head>
<body OnLoad="OnLoadEvent();" >
<form name="mainform" action="acs_url HERE" method="POST">
<noscript>
<br>
<br>
<center>
<h1>Processing your 3-D Secure Transaction</h1>
<h2>
JavaScript is currently disabled or is not supported
by your browser.<br></h2>
<h3>Please click Submit to continue
the processing of your 3-D Secure
transaction.</h3>
<input type="submit" value="Submit">
</center>
</noscript>
<input type="hidden" name="PaReq" value="PaReq HERE">
<input type="hidden" name="TermUrl" value="TERM URL HERE">
<input type="hidden" name="MD" value="MD DATA HERE">
</form>
<SCRIPT LANGUAGE="Javascript" >
<!--
function OnLoadEvent()
{
document.mainform.submit();
}
//-->
</SCRIPT>
</body>
</html>
```

When the cardholder has authenticated themselves, the issuer's ACS will redirect the cardholder back to the TermUrl that the merchant's server supplied. The merchant server will then be required to extract certain information from the redirected form and pass this data to SECPay's MPI for verification. Please refer to the next section for details on how to perform this process.

4.2.3. 3-D Secure Authorisation Request

When the merchant's server has received the redirected ACS HTML form, the merchant's server will then need to extract the parameters as shown in figure 4.9 from the form:

Fig. 4.9: ACS return parameters

Parameter	Description
MD	Unique reference used by all parties including SECPay and the merchant to identify and track the 3-D Secure transaction
PaRes	The Payment Authentication Response that the card issuer users returns after the authentication process

The merchant server software will then need to pass the relevant data to SECPay so the data can be verified and the transaction authorisation can be performed.

A POST should be sent to the following URL:
https://www.secpay.com/ java-bin/XMLMPIValCardPart2

Figure. 4.10, shows a typical 3-D Secure Authorisation request.

Fig 4.10: 3-D Secure Authorisation Request

```
XMLRequest>
        <PaRes>eJxVUu1qgzAU/b
nKD6AiZkftdymRLtBB65lc9D9FA2aUbUzWtzbL0ld6y4E7z2enJx7E9iM9WIx4Z0UbbO2HBtb
G/oAadVxvn3n
dBxCgmXMiv5QhRriwROiEPsLC0KB/bGpUFrWdq3P7YUZcMLRZh0qZK1CaC/Ugl2eZU1P
YUs/452r9QNHT8IAE0l1LzbbSkJiBN4IcHXAHSFAd33HwadSWVyFAVNvvJxnzIv2T65u5iVs
7UGpBlQZD2nStHDPnEWOFi5wYp4gAwOZy3H6nZQ2p6vj5wjoMbR8Sb/oUviA7pVwMdz2
3DFUE3eckB3c
esoXgWLnEVVaOQHin0op6bWmpTj2ocBgfZZ/0g6SegKYM8u1xozFgcjUl6iuLji6jK52j/wa6h
mjUU4LmgWHWnv2YXO5VtJ/qq1lb/A4C0FWQu1czYXLqG54/hF3p6sJ0=</PaRes>
        <MD>271909018</MD>
</XMLRequest>
```

The SECPay MPI decodes the PARes to establish whether the cardholder was authenticated. SECPay's payment gateway will respond with the results of the 3-D Secure authorisation request as shown in figure 4.11. The **mpi_status_code** field indicates the result of the authentication process.

Fig 4.11: 3-D Secure Authorisation Response

```
<XMLResponse>
  <valid>true</valid>
  <trans_id>secpay_xml_test</trans_id>
  <code>A</code>
  <auth_code>986654</auth_code>
  <amount>56.00</amount>
  <hash>18236852b58411975ddfed55b978d4e7</hash>
  <mpi_status_code>237</mpi_status_code>
  <mpi_message>Payer authentication successful (Y)</mpi_message>
</XMLResponse>
```

In general, if the merchant receives a status code as shown in figure 4.12 from the 3-D Secure Authorisation Response, the liability shift offered by 3-D Secure can be obtained except in the case of a MPI status code of 229 - the cardholder failed to be authenticated.

Fig. 4.12: 3-D Secure Payer Verification Required Status Code

MPI Status Code	Description	Action
237	Payer Authenticated	The cardholder was authenticated
236	Authentication Attempt	The issuer ACS returned an Authentication Attempt Response.
229	Not Authenticated	Cardholder was NOT authenticated. Failed Authentication

Any other code indicates that liability shift was not obtained or a processing error occurred in which case no liability shift will be obtained. Please refer to section 3.8 for more information on liability shift and Appendix A for the possible status codes that can be returned by the MPI.

NOTE: The merchant's software should be designed to accommodate future enhancements to SECPay's MPI and allow for additional MPI return codes as and when they are added.

In the case of all MPI status codes, except code 229 which will be failed, SECPay will attempt to authorise the transaction with the acquiring bank, and the result will be returned to the merchant in the format as shown in figure 4.11. The only extra parameters returned are:
mpi_status_code (Refer to Appendix A)
mpi_message (user-friendly description of the status code)

4.3. SECPay SOAP/XML-RPC Gateway Integration

SECPay merchants' interface their systems with SECPay hosted MPI by adding a link to a secured URL. Please refer to the SOAP or XML RPC Integration guide for more information on general information and parameters required.
As part of 3-D Secure, merchants' are required to display logos, similar to those shown below. Please refer to section 3.9 for more information on displaying the logos.

The next two sections describe the steps involved to allow the merchant to successfully integrate SOAP and XML/RPC to perform 3-D Secure authentication.

4.3.1. Three D Secure Enrolment Request

For a 3-D Secure transaction, the merchant's customer enters their details into the merchant's payment page as for a non 3-D Secure transaction. The merchant's website then makes a secure SSL call to SECPay's SOAP or

XML/RPC payment gateway as with a normal payment gateway call. However, with a 3-D Secure transaction, the process is significantly different. The merchant has to make a ***threeDSecureEnrolmentRequest*** to check to see if the cardholder is enrolled for 3-D Secure. The merchant must supply all the mandatory parameters to allow SECPay's MPI to check the enrolment status of the card and, if necessary, generate a PAReq message that is required by the card issuer. The way in which the merchant's software gathers this extra data is not within the scope of this document and it is assumed that your web application can capture and/or generate the required data.

Figure. C.1, Appendix C, shows the extra parameters that are required to perform a 3-D Secure Enrolment request. The data is required to build a PAReq if the cardholder is enrolled for 3-D Secure.

Figure. C.2, Appendix C, shows a typical SOAP 3-D Secure Enrolment request and figure C.5 shows the XML-RPC 3-D Secure Enrolment request. The extra 3-D Secure data is supplied so the SECPay MPI can build a VEReq to establish whether the cardholder is enrolled for 3-D Secure.

SECPay's payment gateways will respond with the results of the enrolment check; Figure C.3 and C.4 for SOAP and figure C.6 and C.7 for XML-RPC of Appendix C. The **mpi_status_code** field indicates what action should be taken next.

In general, after the enrolment request response is received and if the merchant receives one of the status codes as shown in figure 4.12, the liability shift offered by 3-D Secure can be obtained or in the case of a MPI status code of 200, the cardholder has to be redirected to the card issuer and authenticated to gain liability shift. Any other code indicates that liability shift was not obtained or an error occurred in which case no liability shift was obtained. Please refer to section 3.8 for more information on liability shift. Please refer to Appendix A for the possible status codes that can be returned by the MPI.

NOTE: The merchant's software should be designed to accommodate future enhancements to SECPay's MPI and allow for additional MPI return codes as and when they are added.

In the case of all MPI status codes except code 200, SECPay will attempt to authorise the transaction with the acquiring bank, and the result will be returned to the merchant in the format as shown in figure C.4, Appendix C for SOAP and figure

C.7 for XML-RPC. The only extra parameters returned by the SOAP/XML-RPC gateways are:

mpi_status_code (Refer to Appendix A)
mpi_message (user-friendly description of the status code)

Fig. 4.13: 3-D Secure Payer Verification Required Status Code

MPI Status Code	Description	Action
200	Payer Verification Required	The payer should now be redirected to the issuer to be authenticated.
212	Cardholder Not Enrolled	The cardholder is not enrolled for 3-D Secure

4.3.2. 3-D Secure Cardholder Authentication Process

Before 3-D Secure, SECPay returned the result of the authorisation attempt from the merchant's acquiring bank and the merchant displayed the result to the cardholder. However, with the 3-D Secure scheme and if a status code of 200 is returned from SECPay's MPI, the cardholder is required to be authenticated. To enable the cardholder to be authenticated, the cardholder must be redirected to the card issuer via a redirect page. This section shows you how to construct the basic page.

The information that is added to the page are 3 fields returned by the MPI and 1 field added by the merchant's server:

Fig. 4.14: MPI return parameters

Parameter	Description
acs_url*	The URL Encoded URL of the issuer's Access Control Server (ACS) which the cardholder is redirected to. ***This field will need to be URL decoded as SECPay URL Encode this field***
MD*	Unique reference used by all parties including SECPay and the merchant to identify and track the 3-D Secure transaction
PaReq*	The Payment Authentication Request that the card issuer users for the authentication process
TermUrl	TermUrl contains the URL on the merchant's server where the cardholder is redirected to following authentication by the issuer's ACS.

**** These fields are extracted from the SECPay 3-D Secure enrolment response. The acs_url will need to be URL Decoded by the merchant prior to using in the redirect page (figure 4.14)***

When all the necessary data is extracted from the enrolment check response, the merchant's application is required to construct and return a page similar to the one in figure 4.15, which redirects the cardholder's browser to the issuer's ACS. The TermUrl contains the URL on the merchant's server where the cardholder is redirected to following authentication by the issuer's ACS.

Fig. 4.15: 3-D Secure Redirect Page

```
<html>
<head>
<title> 3-D Secure Verification</title>
</head>
<body OnLoad="OnLoadEvent();" >
<form name="mainform" action="acs_url HERE" method="POST">
<noscript>
<br>
<br>
<center>
<h1>Processing your 3-D Secure Transaction</h1>
<h2>
JavaScript is currently disabled or is not supported
by your browser.<br></h2>
<h3>Please click Submit to continue
the processing of your 3-D Secure
transaction.</h3>
<input type="submit" value="Submit">
</center>
</noscript>
<input type="hidden" name="PaReq" value="PaReq HERE">
<input type="hidden" name="TermUrl" value="TERM URL HERE">
<input type="hidden" name="MD" value="MD DATA HERE">
</form>
<SCRIPT LANGUAGE="Javascript" >
<!--
function OnLoadEvent()
{
document.mainform.submit();
}
//-->
</SCRIPT>
</body>
</html>
```

When the cardholder has authenticated themselves, the issuer's ACS will redirect the cardholder back to the TermUrl that the merchant's server supplied. The merchant server will then be required to extract certain information from the redirected form and pass this data to SECPay's MPI for verification. Please refer to the next section for details on how to perform this process.

4.3.3. 3-D Secure Authorisation Request

When the merchant's server has received the redirected ACS HTML form, the merchant's server will then need to extract the parameters as shown in figure 4.16 from the form:

Fig. 4.16 : ACS return parameters

Parameter	Description
MD	Unique reference used by all parties including SECPay and the merchant to identify and track the 3-D Secure transaction
PaRes	The Payment Authentication Response that the card issuer users returns after the authentication process

Depending on the interface used, the merchant will pass the relevant data to SECPay so the data can be verified and the transaction authorisation can be performed.

The ***3-D Secure Authorisation Request*** method is used to send the request from the 3-D Secure authentication process to SECPay's MPI. Figure. C.9, Appendix C for SOAP and C.12 for XML-RPC, show a typical 3-D Secure Authorisation request.

The SECPay MPI decodes the PARs to establish whether the cardholder was authenticated. SECPay's payment gateway will respond with the results of the 3-D Secure authorisation request as shown in figure C.10, Appendix C for SOAP and figure C.12, Appendix C for XML-RPC. The **mpi_status_code** field indicates the result of the authentication process.

In general, if the merchant receives a status code as shown in figure 4.17 from the 3-D Secure Authorisation Response, the liability shift offered by 3-D Secure can be obtained except in the case of a MPI status code of 229 - the cardholder failed to be authenticated.

Fig. 4.17: 3-D Secure Payer Verification Required Status Code

MPI Status Code	Description	Action
237	Payer Authenticated	The cardholder was authenticated
236	Authentication Attempt	The issuer ACS returned an Authentication Attempt Response.
229	Not Authenticated	Cardholder was NOT authenticated. Failed Authentication

Any other code indicates that liability shift was not obtained or a processing error occurred in which case no liability shift will be obtained. Please refer to section 3.8 for more information on liability shift and Appendix A for the possible status codes that can be returned by the MPI.

NOTE: The merchant's software should be designed to accommodate future enhancements to SECPay's MPI and allow for additional MPI return codes as and when they are added.

In the case of all MPI status codes, except code 229 which will be failed, SECPay will attempt to authorise the transaction with the acquiring bank, and the result will be returned to the merchant in the format as shown in figure C.10, Appendix C for SOAP and figure C.12, Appendix C for XML-RPC. The only extra parameters returned are:

mpi_status_code (Refer to Appendix A)
mpi_message (user-friendly description of the status code)

5. 3-D SECURE TRANSACTION REPORTING

SECPay's transaction reporting system has been extended to include details indicating that the transaction has been processed under 3-D Secure.

The merchant can view transactions that have been processed by the 3-D Secure MPI by selecting the Origin Reporting facility (for SECNet users selct the Origin Report from the drop-dopwn list of predefined reports in the Transaction Manager facility). The report shows the 3-D Status, Card Type and card country of issue. The latter two parameters are included because MasterCard SecureCode does not give

liability shift for all MasterCard regions except for “fully Authenticated” transactions. Visa does not give liability shift protection for Visa Commercial Cards (Internationally issued). This is supplied so the merchant can make an informed decision to whether a transaction is protected under the Visa or MasterCard implementation. Please refer to your acquirer documentation for more information on liability shift or the Visa/MasterCard Merchant Implementation Guides.

The table in figure 5 shows the various types of response that can be displayed in the 3D Status field with a brief description. The table also shows the mapped ECI values. These values can be found by drilling-down on the corresponding text link in the 3D Status field. Figure 5.3 shows the MPI Record for a corresponding Authenticated 3-D Secure transaction.

Fig. 5: Guide to 3-D Secure Transaction 3D Status Types

3D-Status	ECI Values (VBV/SecureCode)	Description
Authenticated	5/2	Cardholder successfully authenticated. Issuer generated CAVV.
Not Authenticated	-	Cardholder was NOT authenticated. Failed Authentication.
Cardholder Not Enrolled	6/1	Authentication Attempt but cardholder not enrolled.
Authentication Attempt	6/1	The issuer ACS returned an Authentication Attempt Response.
Authentication Unavailable	-	The issuer ACS returned an Authentication Not Available response.
Unable to Verify Enrolment	-	The VBV or SecureCode DS was unable to verify whether the cardholder was registered.
Merchant Not Participating	-	The VBV or SecureCode Directory Server indicated that the merchant is not registered. Merchants cannot gain liability shift if they are not registered in the scheme. Please contact SECPay for further information if this type of message is received
Other Result	-	This indicates that the MPI encountered another response or an error occurred. The merchant should drill-down to ascertain the exact cause and whether they have liability shift for this transaction

6. SECPAY TEST DIRECTORY SERVER AND ACS SIMULATOR

The SECPay ACS Simulator allows the merchant to fully simulate the 3D-authentication process and the interaction with the VBV or SecureCode Directory Server and the issuing bank ACS. The merchant can send requests and test the responses from the DS and ACS simulator.

To use the SECPay 3-D Secure test simulator, the test_status flag must be passed in the authorisation request. From an html post, this would be included by the following html code:

<input type="hidden" name="test_status" value="true">

Note: Please refer to the SECCard integration guide for valid test_status values

If the merchant is not enabled on the SECPay server to perform 3-D Secure transaction, a test transaction can be performed by using the following option:

test_mpi_status=true

Note: To utilise this option, a valid test_status value of true or false must be included.

6.1. Testing Responses from the Test Directory Server

This allows particular responses to be received from the SECPay test Directory Server. The MPI gateway has been extended to allow certain Enrolment Verification Requests to be obtained. This is achieved by specifying any test card number with an appropriate value for the month in the expiry date field. Please refer to the table in figure 6.1 for the month values and the expected response.

For example, to achieve a Cardholder Not enrolled response, use the following:
Month: 02
Year: 08 (any valid year in the future)

To use the SECPay test Directory Server, the test_status flag must be passed in the authorisation request. From an html post, this would be included by the following html code:

<input type="hidden" name="test_status" value="true">

Note: Please refer to the SECCard integration guide for valid test_status values

If the merchant is not enabled on the SECPay server to perform 3-D Secure transaction, a test transaction can be performed by using the following option:

test_mpi_status=true

Note: To utilise this option, a valid test_status value of true or false must be included.

Fig. 6.1: Test Directory Server Month Values and Expected Response

Month	Response	MPI Code
01	Cardholder Enrolled	200*
02	Not Enrolled	212
03	Unable To Verify Enrolment	234
04	Format Error Response (VERes message from DS)	210
05	Acquirer Not Participating	255
06	Merchant Not Participating	256
07	3D Password Required	257
Other value	Invalid request Error (98)	210

* SECCard service merchants will be redirected to the Test ACS Simulator to begin Authentication Tests – Please refer to next section.

6.2. Testing responses from the ACS Simulator

The ACS simulator allows particular responses to be received from the SECPay ACS Simulator. The MPI gateway has been extended to allow certain Verify Enrolment Request responses to be obtained. This can be achieved by specifying any test card numbers with a value of '01' for the month in the card expiry field.

To use the SECPay 3-D Secure test ACS Simulator, the test_status flag must be passed in the authorisation request. From an html post, this would be included by the following code:

<input type="hidden" name="test_status" value="true">

The following steps show how to connect to the ACS Simulator:

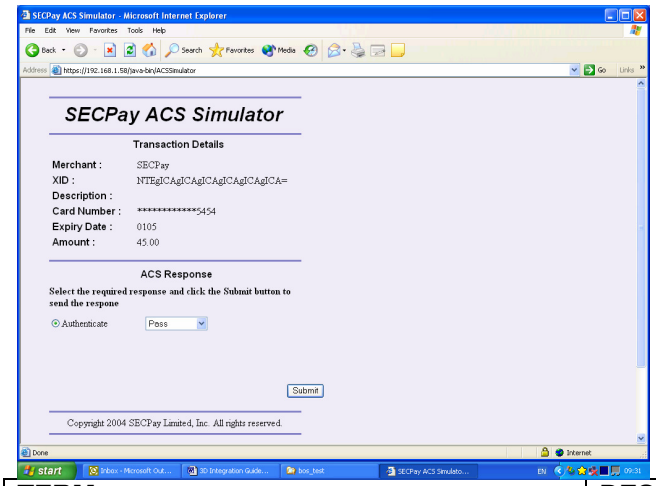
1: On the payment page, enter the usual required details and set the expiry date month to '01' and any valid year in the future: (0108).
2: Submit
3: The ACS Simulator will appear as shown in figure 6.3

Figure 6.2 shows the possible responses that can be generated by selecting the appropriate Authentication drop-down option and clicking the Submit button.

Fig. 6.2: ACS Simulator Options and Responses

Option	Response	MPI Code
Pass	Cardholder Authenticated	237
Fail	Cardholder Not Authenticated	229
Attempt	Authentication Attempt	236
Unavailable	Authentication Unavailable	235

Fig. 6.3: SECPay ACS Simulator



TERM	DESCRIPTION
3-D Secure	3 Domain Secure ecommerce environment including Acquirers/Merchants, issuers/cardholder and Card Schemes.
AAV	Accountholder Authentication Value. Unique reference generated by MasterCard card issuers to prove authentication took place.
Acquirer	A Member financial institution that establishes a contractual service relationship with a merchant for the purpose of accepting payment cards. In 3-D Secure, determines whether merchant is eligible to participate. Performs traditional role of receiving and forwarding authorisation and settlement messages (enters transaction into interchange).
ACS	Access Control Server. Card Issuer system to record which cardholders are registered
CAVV	Cardholder Authentication Verification Value. Unique reference generated by Visa card issuers to prove authentication took place.
DS	Directory Server .A system operated by Visa and MasterCard which determines whether a specific issuer and card number is participating in authentication, and if so, it returns the URL of the appropriate Access Control Server to the Merchant Plug-in.
ECI	ECommerce Indicator. Provides the security level used in an Internet transaction.
European Region	Specific European regions as defined by the card schemes (see Intra-Regional).
In-Line Window	Internet Browser window, within the main browser page.
MPI	Merchant Plug-in. Software module that

TERM	DESCRIPTION
	provides merchants the ability to perform 3-D Secure authentication
PAReq	Payer Authentication Request. 3-D Secure Protocol message type. This is a request sent by the SECPay MPI client to check if a buyer passed 3-D Secure authentication.
PARes	Payer Authentication Response. 3-D Secure Protocol message type. This is the response returned after submitting a PAReq. It indicates whether or not the cardholder passed 3-D Secure authentication.
Pop-Up	Internet Browser Pop Up window, displayed as an extra window.
SecureCode	MasterCard SecureCode. Cardholder authentication scheme from MasterCard.
UCAF	Universal Cardholder Authentication Field. The data field used by MasterCard issuers to send the AAV (see above).
VBV	Verified by Visa. Cardholder authentication scheme from Visa.
VEReq	Verify Enrolment Request. 3-D Secure Protocol message type. This is a request sent by the SECPay MPI client to check if a given credit card number is enrolled on the VBV or SecureCode DS.
VERes	Verify Enrolment Response. 3-D Secure Protocol message type. This is the response returned after submitting a VEReq. It indicates whether or not the credit card number is enrolled in VBV or SecureCode scheme.
XID	The unique transaction identifier.

APPENDIX A: SECPay MPI Return Codes

This section contains details of the possible return codes that can be received from the SECPay MPI software and a description of when the response would be received.

MPI CODE	DESCRIPTION
200	Payer Verification required. The DS indicated that the cardholder is enrolled and should now be authenticated via the issuer's ACS
205	Filed Missing. A field such as merchant_url is missing
207	Merchant is Not Enabled to perform 3-D Secure transactions
208	Card Scheme Not Supported for 3-D Secure transactions
209	The SECPay MPI software has no VERes from directory server
210	Invalid VERes received from the DS
212	Cardholder Not Enrolled
213	The merchant is not enabled for the card scheme with the acquiring bank
214	The SECPay MPI has no DS URL details for the acquirer card scheme
215	The merchant is not enabled to perform 3-D Secure with the acquirer
216	The format of the purchase date/time field supplied in the 3-D Secure enrolment check request is invalid
217	An invalid reference was supplied in the 3-D Secure transaction request
218	The transaction could not be submitted for authorisation because no valid 3-D Secure enrolment check request could be found
222	The required PARes was not supplied in the 3-D Secure Authorisation request for an enrolled card
224	The PARes message digital signature from the issuer could not be verified
225	A PARes message has been received in a 3-D Secure Authorisation request, but no matching PAReq was found
226	The PARes in the 3-D Secure authorisation request is invalid. This occurs when the format of the received XML message is not well-formed
227	The PAReq received from the 3-D Secure enrolment check request is invalid. This occurs when the format of the received XML message is not well-formed
228	The PAReq and PARes do not match on one of the following key fields: message_id, acqBIN, merID, xid, date, purchAmount, currency, or exponent.
229	The PARes message received was valid but the cardholder was not authenticated by the card issuer's ACS.
230	MPI did not receive a PARES from the Directory server for the timeout set
231	The MPI could not connect to the Directory Server
232	An IO Interrupt Occurred whilst connected to the Directory Server
234	VERes indicated unable to verify enrolment
235	PARes indicated that the ACS authentication was not available
236	PARes indicated the ACS returned an authentication attempt
237	PARes indicated authentication was successful
238	An unspecified error occurred when trying to decode the PARes message
239	The merchant Address Information is not set
240	An unspecified error occurred when trying to connect to the DS
241	The merchant information is not set
242	The merchant acquirer information not set
243	The merchant password is required for the scheme but is not set

MPI CODE	DESCRIPTION
244	An IO error occurred whilst connected to the DS
255	Acquirer not participating in 3-D Secure scheme (DS returned error 50)
256	Merchant not participating in 3-D Secure scheme (DS returned error 51)
257	Password not supplied in 3-D Secure VEReq (DS returned error 52)
258	Incorrect password supplied in 3-D Secure VEReq (DS returned error 53)
259	The SECPay MPI is not enabled – 3-D Secure transactions cannot be performed

APPENDIX B: Visa and MasterCard Regions

VISA Regions

There are five regions that make up Visa International: Asia Pacific (AP); Canada; Central and Eastern Europe, Middle East and Africa (CEMEA); Latin America-Caribbean (LAC); and the USA.

VISA EU Region

Visa Europe region represents 26 European countries: Andorra, Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Gibraltar, Greece, Greenland, Iceland, Ireland, Israel, Italy, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey and the UK.
As a result of the EU's political expansion, Visa Europe will have eight more countries joining from Visa CEMEA in October 2004 – Estonia, Czech Republic, Hungary, Latvia, Lithuania, Poland, Slovakia and Slovenia.

NOTE: MERCHANTS MUST refer to their acquirer for correct information regarding Visa's regions. SECPay cannot take responsibility for any incorrect information regarding Visa Regions.

MasterCard Regions

MasterCard is organized geographically into the following regions: Asia/Pacific; Europe; Latin America and Caribbean; North America (U.S. and Canada); and South Asia, Middle East and Africa.

MasterCard EU Region

NOTE: MERCHANTS MUST refer to their acquirer for correct information regarding MasterCard's regions. SECPay cannot take responsibility for any incorrect information regarding MasterCard Regions.

APPENDIX C: 3-D Secure SOAP and XML-RPC Remote Calls

3-D Secure Enrolment Request Parameters

Fig. C.1 3-D Secure enrolment request parameters

Method Name: **SECVPN. threeDSecureEnrolmentRequest**

PARAMETER	EXAMPLE	DEFINITION
mid	secpay	This is your secpay username (usually six letters and two numbers).
vpn_pswd	secpay	Your VPN password can be set from within the Merchant Extranet: https://www.secpay.com/lookup. (Click on "Change Remote Passwords" and select VPN from the drop down list).
trans_id	TRAN0001	A unique transaction identifier created by yourself. This can be used to refer to a transaction at a later date (to refund it for example).
ip	127.0.0.1	The IP address that the cardholders machine is presenting to the internet.
name	Mr Cardholder	The cardholders name as it is on their card.
card_number	4444333322221111	The credit card number (this should contain no spaces or hyphens). The example card number show to the left is a test Visa card which can be used during development. Any valid expiry date which is in the future can be used with this card number.
amount	50.00	The amount for the transaction. This should contain no currency symbols or formatting (for example do not send an amount with a comma in).
expiry_date	0105	The credit card expiry date. Should be formatted either as **mm/yy** or **mmyy**.
issue_number	3	The credit card issue number. This only applies to switch or solo cards. If the card in use does not have an issue number then an empty string should be passed in.
start_date	0102	The credit card start date. If the card does not have a start date then an empty string should used.
order	prod=funny_book,item_amount=18.50x1;prod=sad_book,item_amount=16.50x2	Used to submit order details relevant to this transaction. Please see the User Manual for further details: http://www.secpay.com/sc_api.html#order.

PARAMETER	EXAMPLE	DEFINITION
shipping	name=Fred+Bloggs,company=Online+Shop+Ltd,addr_1=Dotcom+House,addr_2=London+Road,city=Townville,state=Countyshire,post_code=AB1+C23,tel=01234+567+890,fax=09876+543+210,email=somebody%40secpay.com,url=http%3A%2F%2Fwww.somedomain.com	Used to submit shipping address details relevant to this transaction. Please see the User Manual for further details: http://www.secpay.com/sc_api.html#shipping.
billing	name=Fred+Bloggs,company=Online+Shop+Ltd,addr_1=Dotcom+House,addr_2=London+Road,city=Townville,state=Countyshire,post_code=AB1+C23,tel=01234+567+890,fax=09876+543+210,email=somebody%40secpay.com,url=http%3A%2F%2Fwww.somedomain.com	Used to submit billing address details relevant to this transaction. Please see the User Manual for further details: http://www.secpay.com/sc_api.html#billing.
options	test_status=true,dups=false,card_type=Visa	Used to submit optional parameters which are used to alter the behaviour of this transaction. Please see the User Manual for further details: http://www.secpay.com
device_category	0	Indicates the type of device or channel being used for shopping. A value of 0 (zero) indicates a standard web browser; a value of 1 (one) indicates a mobile WAP based browser.
accept_headers	image/gif, image/ x-xbitmap, image/jpeg, image/pjpeg, application/ vnd.ms-excel, application/ vnd.ms-powerpoint, application /msword, application/ x-shockwave-flash, */*	The exact content of the HTTP accept header as sent to the merchant from the cardholder's user agent. Determined from the web server environment.
user_agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)	The exact content of the HTTP user-agent header as sent to the merchant from the cardholder's user agent. Determined from the web server environment.

PARAMETER	EXAMPLE	DEFINITION
mpi_merchant_name	Your Company Name	Merchant Name to be displayed on the authentication page (0 – 125 characters). Required if not using value on SECPay database.
mpi_merchant_url	http://yoururl.com	Fully qualified URL of Merchant website (0 – 2048 characters. Required if not using value on SECPay database
mpi_description	Widgets	Order Description. A brief description of items purchased (0 – 125 characters). Optional. It is advisable to include this field in case of disputes.
purchaseRecurringFrequency	1	Required if the merchant and cardholder have agreed to recurring payments. The minimum number of days between authorizations (0-4 digits)
purchaseRecurringExpiry	20041210	Required if the merchant and cardholder have agreed to recurring payments. Date after which no authorizations should be performed (YYYYMMDD)
purchaseInstallments	2	Maximum number of permitted authorizations for installment payments (0 - 3 digits)

Fig. C.2: Example 3-D Secure SOAP Enrolment Request

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1: threeDSecureEnrolmentRequest
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="SECCardService">
   <ns1:arg0 xsi:type="xsd:string">secpay</ns1:arg0>
   <ns1:arg1 xsi:type="xsd:string">secpay</ns1:arg1>
   <ns1:arg2 xsi:type="xsd:string">TRAN0001</ns1:arg2>
   <ns1:arg3 xsi:type="xsd:string">127.0.0.1</ns1:arg3>
   <ns1:arg4 xsi:type="xsd:string">Mr Cardholder</ns1:arg4>
   <ns1:arg5 xsi:type="xsd:string">4444333322221111</ns1:arg5>
   <ns1:arg6 xsi:type="xsd:string">50.00</ns1:arg6>
   <ns1:arg7 xsi:type="xsd:string">0105</ns1:arg7>
   <ns1:arg8 xsi:type="xsd:string"></ns1:arg8>
   <ns1:arg9 xsi:type="xsd:string"></ns1:arg9>
   <ns1:arg10 xsi:type="xsd:string"></ns1:arg10>
   <ns1:arg11
xsi:type="xsd:string">name=Fred+Bloggs,company=Online+Shop+Ltd,addr_1=Dotcom+Hou
se,addr_2=London+Road,city=Townville,email=somebody@secpay.com</ns1:arg11>
   <ns1:arg12 xsi:type="xsd:string"></ns1:arg12>
   <ns1:arg13
xsi:type="xsd:string">test_status=true,dups=false,card_type=Visa</ns1:arg13>
   <ns1:arg14 xsi:type="xsd:string">0</ns1:arg14>
   <ns1:arg15 xsi:type="xsd:string"> image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-
shockwave-flash, */*</ns1:arg15>
   <ns1:arg16 xsi:type="xsd:string"> Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
.NET CLR 1.0.3705)</ns1:arg16>
   <ns1:arg17 xsi:type="xsd:string"> </ns1:arg17>
   <ns1:arg18 xsi:type="xsd:string"></ns1:arg18>
   <ns1:arg19 xsi:type="xsd:string">Widgets</ns1:arg19>
   <ns1:arg20 xsi:type="xsd:string"></ns1:arg20>
   <ns1:arg21 xsi:type="xsd:string"></ns1:arg21>
   <ns1:arg22 xsi:type="xsd:string"></ns1:arg22>
  </ns1: threeDSecureEnrolmentRequest >
 </soapenv:Body>
</soapenv:Envelope>
```

Fig. C.3: Example 3-D Secure SOAP Enrolment Request Response for Cardholder Authentication required

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1: threeDSecureEnrolmentRequestResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="SECCardService">
   <ns1: threeDSecureEnrolmentRequestReturn
xsi:type="xsd:string">?valid=true&trans_id=TRAN0001&test_status=true&mpi_status_code=
200&mpi_message=Payer Verification required&acs_url
=https%3A%2F%2Fwww.secpay.com%2Fjava-
bin%2FACSSimulator&MD=180527679&PaReq=eJxVUttygjAQfe9XMH6ACVQUnDUO1Xa
Ko0jF9p0JW7UjoAHU/n03CGofMtlzsrs5e4HxJd0bJ1TFLs9GHbPLO2PxBOutQpxGKCuFAh
ZYFPEGjV1CHg63rUF/4HYEhN4KjwKaaEHBXQtYCylMyW2clQJieXzxA9FzLZdzYA2EFJU/
FX3HtG2H6CuELE5RtLFGQAhYzYHMq6xUv8Kx+sBaAJXai21ZHoohY795pQh3ZZ4C0w/A
7irCSlsFJbrsErFYb87B2n8OfqTtT7zNwxkB0x6QxCUKi/OeyS3bMPnQHgy5A6zmIU61AirKd
amkK4CD/sN7fHlkgPqpMJNtCS0CvBzyDMmD+nezIcFCikXoG9PXaLLyw7W/DOh3zcJKz0b
At8JjVecwgd0BYJZcPWr5pkntvVHA2vvekcm7npIsaQA4O8+jiFfR52U5P71x78P72m/CmZ5
b7aDV7qjz3OSDWq4GwHQK1qwEa1aGrH+r9AcmdM2G</ns1:
threeDSecureEnrolmentRequestReturn>
  </ns1: threeDSecureEnrolmentRequestResponse>
 </soapenv:Body>
</soapenv:Envelope>
```

Fig. C.4: Example 3-D Secure SOAP Enrolment Request Response for Cardholder Not Participating

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1: threeDSecureEnrolmentRequestResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="SECCardService">
   <ns1: threeDSecureEnrolmentRequestReturn
xsi:type="xsd:string">?valid=true&trans_id=TRAN0001&code=A&auth_code=9999&amount
=50.0&test_status=true&mpi_status_code=212&mpi_message=Cardholder Not
Participating</ns1: threeDSecureEnrolmentRequestReturn>
  </ns1: threeDSecureEnrolmentRequestResponse>
 </soapenv:Body>
</soapenv:Envelope>
```

Fig. C.5: Example 3-D Secure XML-RPC Enrolment Request

```
<?xml version="1.0"?>
<methodCall>
<methodName>SECVPN. threeDSecureEnrolmentRequest </methodName>
<params>
<param>
<value><string>secpay</string></value>
</param>
<param>
<value><string>secpay</string></value>
</param>
<param>
<value><string>xmltest</string></value>
</param>
<param>
<value><string>123.4.56.789</string></value>
</param>
<param>
<value><string>John Doe</string></value>
</param>
<param>
<value><string>4444333322221111</string></value>
</param>
<param>
<value><string>49.99</string></value>
</param>
<param>
<value><string>01/05</string></value>
</param>
<param>
<value><string></string></value>
</param>
<param>
<value><string>01/02</string></value>
</param>
<param>
<value><string>prod=funny_book,item_amount=18.50;prod=sad_book,item_amount=16.50x
3</string></value>
</param>
<param>
<value><string>name=CONTACT,company=COMPANY,addr_1=ADDRESSLINE1,post_co
de=POST_CODE,tel=TELEPHONE,email=EMAIL,url=URL</string></value>
</param>
<param>
<value><string>name=CONTACT,company=COMPANY,addr_1=ADDRESSLINE1,addr_2=
ADDRESSLINE2,city=CITY,state=COUNTY,country=COUNTRY,post_code=POST_CODE,t
el=TELEPHONE,email=EMAIL,url=URL</string></value>
</param>
<param>
<value><string>test_status=true</string></value>
</param>
<param>
<value><string>0</string></value>
```

```
</param>
<param>
<value><string>image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash,
*/*</string></value>
</param>
<param>
<value><string>Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR
1.0.3705)</value>
</param>
<param>
<value><string></string></value>
</param>
<param>
<value><string></string></value>
</param>
<param>
<value><string>Widgets</string></value>
</param>
<param>
<value><string></string></value>
</param>
<param><value><string></string></value>
</param>
<param>
<value><string></string></value>
</param>
</params>
</methodCall>
```

Fig. C.6: Example 3-D Secure XML-RPC Enrolment Request Response for Cardholder Authentication required

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<methodResponse>
<params>
<param>
<value>?valid=true&trans_id=xmltest&mpi_status_code=200&mpi_message=Payer
Verification required&acs_url=https%3A%2F%2Fwww.secpay.com%2Fjava-
bin%2FACSSimulator
&MD=180560631&PaReq=eJxVUttygjAQfe9XMH6ASVDxMmscqu0UpyIV25k+MrBVOwIaQPHvu0F
Q+5DJnpPdzdkLTMp4b5xQZbs0GbdEm7cm8gnWW4U48zEsFEpYYJYFGzR2EXkMeM/iVke0JHj2Co
8S6mhJwW0TWAMpTIXbIMklBOHx2XFld2gOOQdWQ4hROTNpDUSvNyD6CiEJYpRNrOESAlZxEKZFk
quLHJgWsAZAofZym+eHbMTYJS0U4XaYxsD0A7C7Cq/QVkaJyl0kF+vN2V1/n93fRelM7c3DGQPT
HhAFOUqT867gpmWIzoj3R6YAVvEQxFoBFTUcUklXAAf9h/348sgA9VNhEjYlNAiwPKQJkgf172Z
DhFkoF55jzF786crx1s7Spd81Cys9Gwk/Co9FlYN03QFgEl09KvlCUHtvFLDmvndk+qanFOY0AJ
yf332fF/5nuXw/vXL7w/7ab7y5nlvloNXuqPNc8H4lVwNgOgWrV4LVK0PWv1X6A7WQzfI=</val
ue>
</param>
</params>
</methodResponse>
```

Fig. C.7: Example 3-D Secure XML-RPC Enrolment Request Response for Cardholder Not Participating

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<methodResponse>
<params>
<param>
<value>?valid=true&trans_id=xmltest&code=A&auth_code=9999&amount=49.99&test_statu
s=true&mpi_status_code=212&mpi_message=Cardholder Not Participating</value>
</param>
</params>
</methodResponse>
```

Fig. C.8: 3-D Secure Authorisation request parameters

Method Name: **SECVPN.threeDSecureAuthorisationRequest**

PARAMETER	EXAMPLE	DEFINITION
mid	secpay Bottom of Form	This is your secpay username (usually six letters and two numbers).
vpn_pswd	secpay	Your VPN password can be set from within the Merchant Extranet: https://www.secpay.com/lookup. (Click on "Change Remote Passwords" and select VPN from the drop down list).
trans_id	TRAN0001	A unique transaction identifier created by yourself. This can be used to refer to a transaction at a later date (to refund it for example).
md	271892429	Unique reference used by all parties including SECPay and the merchant to identify and track the 3-D Secure transaction.
paRes	eJxVUm1zgjAM	The Payment Authentication Response that the card issuer builds and returns after the authentication process.
options	N/A	Used to submit optional parameters which are used to alter the behaviour of this transaction. This parameter is included to accommodate future enhancements and is not utilised at the present time

Fig. C.9: Example 3-D Secure SOAP Authorisation Request

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1: threeDSecureAuthorisationRequest
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="SECCardService">
   <ns1:arg0 xsi:type="xsd:string">secpay</ns1:arg0>
   <ns1:arg1 xsi:type="xsd:string">secpay</ns1:arg1>
   <ns1:arg2 xsi:type="xsd:string">TRAN0001</ns1:arg2>
   <ns1:arg3 xsi:type="xsd:string">271892429</ns1:arg3>
   <ns1:arg4
xsi:type="xsd:string">eJxVUm1zgjAM/r5fwfkDbMvYFC92x2S74fnCZNt3rmTqJqAFHP77pQj
T9a7XPE+TNH0SeKjTnXVEXWzzbNwTfd57kDfwttGIfoSq0ihhjkURr9HaJuOePRBD13Zstyc
h9FZ4kNBGSwru28A6SGFabeKslBCrw2OwkJyW49ou58BaClLUgS/vh2LIb++BnSFkcYqyi7
cWhIA1HKi8ykp9kkObvDsAld7JTVnuixFjp7zShPsqT4GZC2CXSsLKWAUlqreJnH+peul/nxZ
+cBdMvPXVHgMzHpDEJUqb6hbcvrOEM3JuR3wArOEhTk0F0nFdl750BrA3b3jXN9cMkKYa
M9V9oUOA9T7PkDxIwz8bEiyUnIeB5T9Fk1UQvgXLBb1uWFiZ/kj41HiomhwC2AUAZsnZoyl
fCFL9jwLWnRdFJi+mU6qkBuD0ZxZFvIre6+Xs+My9V+9jtw6npm+Ng6l2S8pzYcRoATCTgr
VjwdqxIevfOP0CbkfObg==</ns1:arg4>
   <ns1:arg5 xsi:type="xsd:string"></ns1:arg5>
  </ns1: threeDSecureAuthorisationRequest >
 </soapenv:Body>
</soapenv:Envelope>
```

Fig. C.10: Example 3-D Secure SOAP Authorisation Request Response for Cardholder Authenticated

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1: threeDSecureAuthorisationRequestResponse
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="SECCardService">
   <ns1: threeDSecureAuthorisationRequestReturn
xsi:type="xsd:string">?valid=true&trans_id=TRAN0001&code=A&auth_code=9999&amount
=50.0&test_status=true&mpi_status_code=237&mpi_message=Payer authentication
successful (Y)</ns1: threeDSecureAuthorisationRequestReturn>
  </ns1: threeDSecureAuthorisationRequestResponse>
 </soapenv:Body>
</soapenv:Envelope>
```

Fig. C.11: Example 3-D Secure XML-RPC Authorisation Request

```
<?xml version="1.0"?>
<methodCall>
<methodName>SECVPN.threeDSecureAuthorisationRequest</methodName>
<params>
<param>
<value><string>secpay</string></value>
</param>
<param>
<value><string>secpay</string></value>
</param>
<param>
<value><string>xmltest</string></value>
</param>
<param>
<value><string>271892429</string></value>
</param>
<param>
<value><string>eJxVUm1zgjAM/r5fwfkDbMvYFC92x2S74fnCZNt3rmTqJqAFHP77pQjT9a7X
PE+TNH0SeKjTnXVEXWzzbNwTfd57kDfwttGIfoSq0ihhjkURr9HaJuOePRBD13Zstych9FZ4kNB
GSwru28A6SGFabeKslBCrw2OwkJyW49ou58BaClLUgS/vh2LIb++BnSFkcYqyi7cWhIA1HKi8yk
p9kkObvDsAld7JTVnuixFjp7zShPsqT4GZC2CXSsLKWAUlqreJnH+peul/nxZ+cBdMvPXVHgMzH
pDEJUqb6hbcvrOEM3JuR3wArOEhTk0F0nFdl750BrA3b3jXN9cMkKYaM9V9oUOA9T7PkDxIwz8b
EiyUnIeB5T9Fk1UQvgXLBb1uWFiZ/kj41HiomhwC2AUAZsnZoylfCFL9jwLWnRdFJi+mU6qkBuD
0ZxZFvIre6+Xs+My9V+9jtw6npm+Ng6l2S8pzYcRoATCTgrVjwdqxIevfOP0CbkfObg==</stri
ng></value>
</param>
<param>
<value><string></string></value>
</param>
</params>
</methodCall>
```

Fig. C.12: Example 3-D Secure XML-RPC Authorisation Request Response for Cardholder Authenticated

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<methodResponse>
<params>
<param>
<value>?valid=true&trans_id=xmltest&code=A&auth_code=9999&amount=49.99&test_status=true&mpi_status_code=237&mpi_message=Payer authentication successful (Y )</value>
</param>
</params>
</methodResponse>
```