XML Specification: 3-D Secure

This document outlines how to perform Verified by Visa or Mastercard SecureCode transactions (more commonly known as 3-D Secure) with Secure Trading.

Published: 10 January 2018
### Table of Contents

1 Introduction ................................................................................................................................. 3  
   1.1 Internet Merchant Account .................................................................................................. 3  
   1.2 Merchant Plug-In (MPI) ....................................................................................................... 3  
2 Process Overview .......................................................................................................................... 4  
   2.1 Summary of Requests and Responses .................................................................................. 5  
3 3-D Query ..................................................................................................................................... 8  
   3.1 3-D Query XML Request ...................................................................................................... 8  
   3.2 3-D Query XML Response .................................................................................................... 12  
4 Access Control Server (ACS) ...................................................................................................... 16  
   4.1 Referencing 3-D Secure Transactions .................................................................................. 17  
   4.2 Waiting for the customer to return from the ACS ................................................................. 17  
5 Authorisation .................................................................................................................................. 18  
   5.1 3-D Authorisation XML Request ......................................................................................... 18  
   5.2 3-D Authorisation XML Response ........................................................................................ 22  
6 Using your own MPI ......................................................................................................................... 28  
   6.1 Pre-requisites ....................................................................................................................... 28  
   6.2 Enrolled and Authenticated Cards ....................................................................................... 28  
   6.3 Not-Enrolled Cards .............................................................................................................. 30  
   6.4 Authorisation Response ....................................................................................................... 30  
7 Testing............................................................................................................................................ 31  
   7.1 Testing THREEDQUERY ....................................................................................................... 31  
   7.2 Testing ACS (if card is enrolled) .......................................................................................... 32  
   7.3 Testing AUTH ...................................................................................................................... 32  
   7.4 Additional Notes ................................................................................................................... 33  
8 Further Information and Support ................................................................................................ 34  
   8.1 Secure Trading Support ......................................................................................................... 34  
   8.2 Secure Trading Sales ............................................................................................................. 34  
   8.3 Useful Documents .................................................................................................................. 34  
   8.4 Frequently Asked Questions ................................................................................................. 34  
9 Appendix ..................................................................................................................................... 35  
   9.1 PANs to test authorisation ..................................................................................................... 35  
   9.2 PANs to test decline ............................................................................................................... 35  
   9.3 Additional Requests .............................................................................................................. 36
1 Introduction

3-D Secure is a protocol designed to reduce fraud and chargebacks during e-commerce Internet transactions. Cardholders are asked to identify themselves at the point of sale before the purchase can be completed. This usually means entering a PIN or other password after entering their card details.

In the event of a dispute with the transaction at a later date, the card issuer will usually take responsibility of the chargeback instead of the merchant. The liability issues involved with 3-D Secure transactions are outside of the scope of this document. For a detailed indication of the liabilities involved, contact your acquiring bank.

Please note that Secure Trading only supports Mastercard SecureCode and Verified by Visa.

1.1 Internet Merchant Account

You will need to ensure that your Internet Merchant Number or Merchant ID is configured to perform 3-D Secure. This process differs depending on your acquiring bank. For further information, please contact our Support team (see section 8.1).

1.2 Merchant Plug-In (MPI)

The merchant plug-in (MPI) is a software module that is involved in part of the 3-D Secure process. The MPI identifies the customer’s card details and contacts the card issuer to determine if the card is enrolled in a 3-D Secure scheme. If enrolled, the MPI returns the address of the card issuer’s Access Control Server (ACS). The merchant redirects the customer’s browser to the ACS to verify their identity. This process is explained later in this document.

Secure Trading has their own MPI implementation that can be utilised by merchants. This document explains how to configure your system to do this. However, if you already have your own MPI configured as part of your solution, follow the process explained in section 6.
2. Process Overview

The following is a diagrammatic overview of processing payments using 3-D Secure:

1. Customer opts to make a payment on the merchant’s website. The merchant submits a 3-D query request to Secure Trading, including the customer’s card details.

2. Secure Trading interprets the request from the merchant and contacts the card issuer to establish if the customer’s card is enrolled in their 3-D Secure scheme.

3. The merchant receives a 3-D query response from Secure Trading.

4. Is the card enrolled in the 3-D Secure scheme?
   - Yes (enrolled)
     - Merchants redirects the customer to the Access Control Server (ACS), using the URL returned in the 3-D query response.
     - The customer enters information to validate their identity (e.g., password) on the card issuer’s ACS; then the customer is redirected to the merchant’s website.
     - The merchant submits an authorisation request to Secure Trading, including fields returned from the card issuer’s ACS.
     - Was the customer successfully authenticated on the ACS?
       - Yes
         - Secure Trading interprets the request from the merchant and returns a “cardholder not authenticated” response.
       - No
         - The merchant interprets the authorisation response from Secure Trading and displays a success/failure page to the customer.
   - No (not enrolled)
     - The merchant submits an authorisation request to Secure Trading, including transaction reference returned in the 3-D query response.
     - Secure Trading interprets the request from the merchant and seeks authorisation from the merchant’s acquiring bank; then submits a response to the merchant.
2.1 Summary of Requests and Responses

When processing 3-D Secure transactions, your system will need to process the following:

- Submit 3-D query requests and interpret corresponding responses.
- For enrolled cards, redirect the customer’s web browser to the card issuer’s Access Control Server (ACS) and handle the customer when they are redirected back to your server.
- Submit authorisation requests and interpret corresponding responses.

The following diagrams provide an overview of the sequence of requests and responses used in the 3-D Secure process and the important 3-D Secure fields that are included.

The merchant (represented by the grey box on the left) sends requests including the compulsory fields shown (e.g. for the 3-D query request, the Term URL) and receives responses containing the fields shown.

2.1.1 For enrolled cards (Enrolled = ‘Y’)

**MERCHAND**

3-D Query Request

<table>
<thead>
<tr>
<th>INCLUDING FIELDS:</th>
<th>Term URL</th>
</tr>
</thead>
</table>

3-D Query Response

<table>
<thead>
<tr>
<th>INCLUDING FIELDS:</th>
<th>ACS URL</th>
<th>MD</th>
<th>PaReq</th>
</tr>
</thead>
</table>

**secure/trading**

Enrolled = ‘Y’

3-D Query

Your system will need to send a 3-D query request (including the customer's card details) and interpret the response returned.

See section 3.

**VISA**

Access Control Server (ACS)

Your system will need to redirect the customer to the ACS URL and handle the customer being redirected to your Term URL.

See section 4.

**secure/trading**

AUTH Request

<table>
<thead>
<tr>
<th>INCLUDING FIELDS:</th>
<th>MD</th>
<th>PaRes</th>
</tr>
</thead>
</table>

AUTH Response

You will need to send an authorisation request and interpret the response returned.

See section 5.

Key of the fields shown can be found on page 7.
2.1.2 For not-enrolled cards (Enrolled = ‘N’) or unknown enrolment (Enrolled = ‘U’)

In this case, your system will process an authorisation request to STPP immediately after receiving the 3-D query response, ensuring the parent transaction reference and site reference fields are included.

Key of the fields shown can be found on page 7.
2.1.3 Key of important fields

**Enrolled**

The value of the Enrolled field returned in the 3-D query response is used to determine whether or not a card is enrolled in the card issuer’s 3-D Secure scheme:
- ‘Y’ - Card is enrolled.
- ‘N’ - Card is not enrolled.
- ‘U’ - Unable to determine if card is enrolled.

**Term URL**

This field value is a URL of a script/file located on your system that is able to manage customers who are returned to your system. It is used to instruct the card issuer where to send the customer’s browser after they have been authenticated on the card issuer’s ACS.

**MD**

This is a unique reference for the 3-D Secure transaction. It is provided in the 3-D query response if the card is enrolled in the card issuer’s 3-D Secure scheme, and must be included in the subsequent HTTPS POST to the ACS and authorisation request.

The **md** field must remain unaltered throughout the life-cycle of a transaction, otherwise this may forfeit the liability shift.

**ACS URL**

The URL of the card issuer’s ACS. Your system will need to send the customer's browser to this URL using a HTTPS POST, to allow them to perform authentication on the card issuer's ACS (explained in section 4).

**PaReq**

The authentication request for the 3-D Secure transaction. When sending the customer’s browser to the card issuer’s ACS, your system will need to include the PaReq in the HTTPS POST.

**PaRes**

The authentication response for the 3-D Secure transaction. It is used by Secure Trading to determine whether or not the customer has been authenticated by the card issuer. You must include it in your final authorisation request to STPP (if the card is enrolled).

**Transaction Reference**

All responses returned from STPP contain a Transaction Reference. This is used to uniquely identify the transaction submitted.

When the card is not enrolled, your system must take the Transaction Reference from the 3-D query response, and submit it in the Parent Transaction Reference field of the authorisation request to STPP.

This is used to inherit the information needed to process the transaction from the previously-submitted request.
3-D queries are used to determine whether or not the customer’s card is enrolled in the card issuer’s 3-D Secure scheme. This is performed by submitting an XML Request to STPP and interpreting the response returned.

Please note that the ACS URL, MD and PaReq fields are only returned in a 3-D query response for enrolled cards.

Secure Trading allows you to use your own MPI (or use a third-party MPI) to determine if a card is enrolled in the card issuer’s 3-D Secure scheme. See section 6 for further information.

3.1 3-D Query XML Request

This section documents how to construct a 3-D query XML Request. The XML request for a 3-D query is similar to that of a standard e-commerce authorisation (AUTH) request, as described in the XML specification document.

The differences are outlined in this section of the document. The following is a diagrammatic summary of the XML structure required for this request:
3.1.1 <request type = "THREEDQUERY">
The request type is “THREEDQUERY”.

3.1.2 <merchant>
Within the <merchant> tag of your XML Request, there is one additional element required:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>merchant</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>termurl</td>
<td>an</td>
<td>1024*</td>
<td>Y</td>
<td>Term URL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Once the cardholder has verified their identity on the card issuer’s ACS, they will be returned to your server using the URL provided here.

The Term URL must be fully qualified; e.g. https://www.merchant.com/transaction

Secure Trading recommends using a secure URL (i.e. “https://” instead of “http://”). Failing to do so may cause insecure connection warnings in the customer’s browser.

*Note: Certain ACS which do not strictly follow the 3-D Secure specification only allow 255 characters to be submitted, therefore if you are experiencing issues with the length of the Term URL we would suggest reducing it to be under 255 for these ACS.

In the interest of security, it is imperative that you do not pass additional custom fields (such as your own reference) in the Term URL, as this may leave your system more open to field manipulation by the customer/unauthorised third party.

3.1.3 <customer>
Within the <customer> tag of your XML Request, please consider the following fields.

The <accept> element is required.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>accept</td>
<td>an</td>
<td>1024</td>
<td>Y</td>
<td>The exact content of the HTTP accept-header field as received from the cardholder’s user agent.</td>
</tr>
<tr>
<td>useragent</td>
<td>an</td>
<td>255</td>
<td>N</td>
<td>The exact content of the HTTP user-agent header field as received from the cardholder’s user agent. We strongly recommend you submit this field, as failure to do so may forfeit the liability shift.</td>
</tr>
</tbody>
</table>
3.1.4  `<billing>`

Within the `<billing>` tag of your XML Request, your system will need to include the customer’s card details (as with a regular Authorisation request).

Secure Trading also recommends including the billing premise, postcode and security code, to allow the acquiring bank to perform Address Verification System (AVS) and security code checks. For further information, please refer to the [AVS & CVV2 document](#).

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>billing</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>postcode</td>
<td>an</td>
<td>25</td>
<td>N</td>
<td>The postcode entered for the customer’s billing address.</td>
</tr>
<tr>
<td>premise</td>
<td>an</td>
<td>25</td>
<td>N</td>
<td>The house number or first line of the customer’s billing address.</td>
</tr>
<tr>
<td>payment</td>
<td>an</td>
<td>20</td>
<td>Y</td>
<td>The customer’s card type, for example VISA or MASTERCARD.</td>
</tr>
<tr>
<td>type = “”</td>
<td>n</td>
<td>12-19</td>
<td>Y</td>
<td>This is the card number printed on the front of the customer’s card.</td>
</tr>
<tr>
<td>expirydate</td>
<td>an</td>
<td>7</td>
<td>Y</td>
<td>The expiry date printed on the card.</td>
</tr>
<tr>
<td>security</td>
<td>n</td>
<td>4</td>
<td>N</td>
<td>These relate to the three digit security code printed on the back of the</td>
</tr>
<tr>
<td>code</td>
<td></td>
<td></td>
<td></td>
<td>card.</td>
</tr>
</tbody>
</table>

3.1.5  `<operation>`

Within the `<operation>` tag of your XML Request, please ensure your system includes the following fields (as with a regular Authorisation request).

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>operation</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>accounttype</td>
<td>an</td>
<td>20</td>
<td>Y</td>
<td>The value should be “ECOM” (indicating an e-commerce transaction).</td>
</tr>
<tr>
<td>description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sitereference</td>
<td>an</td>
<td>50</td>
<td>Y</td>
<td>The site reference relating to your individual account which you received on setup. If you do not know your Site Reference, please contact Support (see section 8.1).</td>
</tr>
<tr>
<td>authmethod</td>
<td>an</td>
<td>5</td>
<td>N</td>
<td>Either “PRE” or “FINAL”. See section 3.1.5.1 for further information.</td>
</tr>
</tbody>
</table>
3.1.5.1 For Mastercard and Maestro payments

Mastercard Europe have mandated that Mastercard and Maestro transactions processed with certain European acquiring banks must be flagged as either pre-authorisation or final authorisation.

By default, all authorisations meeting these criteria are processed by Secure Trading as final authorisations. However, this can be overridden on an individual transaction by submitting <authmethod> in the <operation> tag, with either “PRE” indicating pre-authorisation or “FINAL” indicating final authorisation.

If successfully submitted in a THREEDQUERY XML Request, the same value will be returned in the THREEDQUERY XML Response and inherited in future child AUTH XML Requests. Secure Trading recommends reading the full guide to the mandate, which can be found in the appendix of the XML Specification document.

3.1.6 XML Request Example

This following is an example of a THREEDQUERY XML Request to be submitted to Secure Trading’s systems (fields specific to 3-D Secure are highlighted in bold).

It contains the fields recommended for inclusion in 3-D query requests, as described previously in this section. You may submit other fields defined in the AUTH XML Request section of the XML Specification document.

```xml
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
  <alias>test_site12345</alias>
  <request type="THREEDQUERY">
    <merchant>
      <orderreference>test.xml.threedquery</orderreference>
      <termurl>https://example.com/termurl.cgi?x=y&amp;b=2</termurl>
    </merchant>
    <customer>
      <useragent>Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.11) Gecko/20071204 Ubuntu/7.10 (gutsy) Firefox/2.0.0.11</useragent>
      <accept>text/html,*/*</accept>
    </customer>
    <billing>
      <amount currencycode="USD">100</amount>
      <postcode>TE45 6ST</postcode>
      <premise>789</premise>
      <payment type="VISA">
        <expirydate>10/2031</expirydate>
        <securitycode>123</securitycode>
        <pan>411111000000211</pan>
      </payment>
    </billing>
    <operation>
      <sitereference>test_site12345</sitereference>
      <accounttypedescription>ECOM</accounttypedescription>
      <authmethod>FINAL</authmethod>
    </operation>
  </request>
</requestblock>
```
### 3.2 3-D Query XML Response

This section documents how to interpret a 3-D query XML Response, which is used to indicate whether or not the customer’s card is enrolled in the card issuer’s 3-D Secure scheme. The XML response for a 3-D query is similar to that of a standard e-commerce authorisation (AUTH) response, as described in the [XML specification document](#). The differences are outlined in this section of the document.

**Please note** that the response outlined in this section only relates to successful requests. Failed requests will return an XML Response containing an `<error><code>` value that is not ‘0’.

Further information on error codes employed by Secure Trading can be found at the following URL: [http://webapp.securetrading.net/errorcodes.html](http://webapp.securetrading.net/errorcodes.html)
### 3.2.1  <response type="THREEQUERY">

The response type is “THREEQUERY”.

### 3.2.2  <threedsecure>

An additional tag `<threedsecure>` is returned in the XML response:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>threedsecure</td>
<td></td>
<td></td>
<td>Y</td>
<td>The unique identifier for the transaction, assigned by the MPI (Merchant Plug-In) (in this case, Secure Trading).</td>
</tr>
<tr>
<td>xid</td>
<td>an</td>
<td>255</td>
<td>Y</td>
<td>Determines if the cardholder is enrolled in a 3-D Secure scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>‘Y’ - Card is enrolled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>‘N’ - Card is not enrolled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>‘U’ - Unable to determine if card is enrolled.</td>
</tr>
<tr>
<td>enrolled</td>
<td>an</td>
<td>1</td>
<td>Y</td>
<td>The URL of the Access Control Server (ACS) to be used in authenticating the cardholder.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Supplied if <code>&lt;enrolled&gt;</code> is ‘Y’.</td>
</tr>
<tr>
<td>acsurl</td>
<td>an</td>
<td>1024</td>
<td>C*</td>
<td>The unique 3-D Secure reference for this transaction.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Supplied if <code>&lt;enrolled&gt;</code> is ‘Y’.</td>
</tr>
<tr>
<td>md</td>
<td>an</td>
<td>1024</td>
<td>C*</td>
<td>The 3-D authentication request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Supplied if <code>&lt;enrolled&gt;</code> is ‘Y’.</td>
</tr>
<tr>
<td>pareq</td>
<td>an</td>
<td>2048</td>
<td>C*</td>
<td>The unique identifier for the transaction, assigned by the PCI (Payment Card Industry) (in this case, Secure Trading).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The URL of the Access Control Server (ACS) to be used in authenticating the cardholder.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Supplied if <code>&lt;enrolled&gt;</code> is ‘Y’.</td>
</tr>
</tbody>
</table>
3.2.3 XML Response Example

Please find below an example of a THREEDQUERY XML Response that is returned from STPP (3-D Secure elements highlighted in **bold**):

```xml
<?xml version="1.0" encoding="utf-8"?>
<responseblock version="3.67">
  <requestreference>X131531678</requestreference>
  <response type="THREEDQUERY">
    <merchant>
      <merchantname>Test Merchant</merchantname>
      <orderreference>test.xml.threedquery</orderreference>
      <tid>00000000</tid>
      <merchantnumber>00000000</merchantnumber>
      <merchantcountryiso2a>GB</merchantcountryiso2a>
      <operatorname>test_site12345</operatorname>
    </merchant>
    <transactionreference>17-33-1</transactionreference>
    <billing>
      <payment type="VISA">
        <issuercountry>US</issuercountry>
        <pan>411111#####0211</pan>
        <issuer>SecureTrading Test Issuer1</issuer>
      </payment>
      <dcc enabled="0"/>
    </billing>
    <timestamp>2014-06-03 09:35:11</timestamp>
    <threedsecure>
      <acsurl>https://webapp.securetrading.net/acs/visa.cgi</acsurl>
      <md>Qzl3WVc1TVpXNW5kR2crUEcxbGMzMhMl2KWWkq1UWFWSmU+jUzB4TWPnNU
      …SXcKtmpxNU5W7thMjFeYzNoAfoYvKpRDQ4TDAxRVbq3EZZVErOmlkUH14R</md>
      <xid>VEw4TkFrakFymEreXdoZE5xZUU==</xid>
      <pareq>eJxVUltpgzAU/itEE32S0nIZzEONu10Ubo4oCt1Mn+vs2yW5/sf9k
      …xGkJ0yb7p3T1pM0fa4CVYNLpTrqfoq2zZh/QHgGHB</pareq>
      <enrolled>Y</enrolled>
    </threedsecure>
    <live>0</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
  </response>
</responseblock>
```

Please note that the `<md>` and `<pareq>` elements typically contain values far longer than displayed in the example above and therefore have been abbreviated using ‘…’, for your convenience.
3.2.4 Managing 3-D Query Response

You will need to interpret the 3-D query response in order to determine how to proceed with the payment.

3.2.4.1 Check the error code

Your system will need to check the error code in the response. If the value returned is not '0', an error has occurred. If an error has occurred when performing a 3-D query, correct the error if possible, by consulting the table below:

<table>
<thead>
<tr>
<th>Error code</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Request was successful.</td>
<td>Check if the card is enrolled by moving on to section 3.2.4.2.</td>
</tr>
<tr>
<td>30000</td>
<td>Invalid field.</td>
<td>Resolve invalid fields highlighted in the XML Response.</td>
</tr>
<tr>
<td>60031</td>
<td>The 3-D query request used a payment type that is not supported by Secure Trading 3-D Secure.</td>
<td>Please submit a regular AUTH XML Request as outlined in the XML Specification.</td>
</tr>
<tr>
<td>Other</td>
<td>Other errors will require further investigation.</td>
<td>Please consult the following URL for a full list of error codes used by STPP: <a href="http://webapp.securetrading.net/errorcodes.html">http://webapp.securetrading.net/errorcodes.html</a></td>
</tr>
</tbody>
</table>

If you are unable to resolve the issue, you can instruct your system to perform a standard AUTH without using 3-D Secure* (see XML Specification).

*Performing a standard authorisation without 3-D Secure will result in forfeiting the liability shift.

For further assistance, please contact Secure Trading Support (see section 8.1) with information about the failed request.

3.2.4.2 Check the <enrolled> element

<table>
<thead>
<tr>
<th>Enrolled</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>The card is enrolled in the card issuer’s 3-D Secure scheme.</td>
<td>Send the customer to the card issuer’s Access Control Server (ACS) (see section 4). The URL for the ACS is provided in the &lt;acsurl&gt; of the 3-D query response.</td>
</tr>
<tr>
<td>N</td>
<td>The card is not enrolled in the card issuer’s 3-D Secure scheme.</td>
<td>Perform a standard AUTH XML Request, including the transaction reference returned in the 3-D query response (see section 5.1.2) as the &lt;parenttransactionreference&gt;.</td>
</tr>
<tr>
<td>U</td>
<td>The card’s enrolment in the card issuer’s 3-D Secure scheme could not be determined.</td>
<td>This typically indicates a temporary problem with the card issuer’s systems. You can configure your system to re-submit the same 3-D query request. If this continues to fail, perform a standard AUTH Request, including the transaction reference returned in the 3-D query response (see section 5.1.2) as the &lt;parenttransactionreference&gt;.</td>
</tr>
</tbody>
</table>
If the customer is enrolled in the card issuer’s 3-D Secure scheme, your system must send the customer’s browser to the card issuer-hosted ACS using an HTTPS POST. The URL for the ACS can be found in the `<acsurl>` element of the 3-D query XML Response.

On the ACS, the customer will be authenticated, typically by providing a previously agreed PIN and/or password.

The browser must send data from the elements `<termurl>`, `<pareq>` and `<md>` in html fields ‘TermUrl’, ‘PaReq’ and ‘MD’, respectively. **These field names are case sensitive.**

Please note that the size of the ACS page displayed in the customer’s browser is controlled by the ACS provider (cannot be modified by merchants or Secure Trading).

As a guideline, Visa US states that the Verified by Visa authentication window should be 390x400 pixels in size.
The following is an example of how to redirect the cardholder to the card issuer’s ACS (the required fields discussed previously have been highlighted in **bold**):

```html
<!DOCTYPE html PUBLIC '-//W3C//DTD HTML 4.01//EN'>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=iso-8859-1">
<title>Processing payment</title>
<style type="text/css">
    h3, h3, h4 { font-family: verdana, arial, sans-serif; font-weight: normal; }
    #logo { float: left; }
</style>
</head>
<body Oncall="document.form.submit();" >
<form name="form" id="form" action="$acsurl" method="POST">
    <input type="hidden" name="PaReq" value="$pareq" />
    <input type="hidden" name="TermUrl" value="$termurl" />
    <input type="hidden" name="MD" value="$md" />
</form>
<noscript>
    <div>
        <h3>JavaScript is currently disabled or is not supported by your browser.</h3>
        <h4>Please click Submit to continue processing your 3-D Secure transaction.</h4>
        <input type="submit" value="Submit">
    </div>
</noscript>
</form>
</body>
</html>
```

The example shown assumes your system will assign the values of the ACS URL, PaReq, Term URL and MD to the variables $acsurl, $pareq, $termurl and $md, respectively.

### 4.1 Referencing 3-D Secure Transactions

In most circumstances, your system will need to store data about the transaction in your database while the customer is being authenticated on the card issuer's ACS, to be retrieved when the customer returns to your system via the Term URL. As the 3-D Secure specification requires that only the MD and PaRes fields are returned to your system, it is recommended that the MD field is used to look up any corresponding customer session to complete the transaction.

### 4.2 Waiting for the customer to return from the ACS

Your system will need to consider the length of time it may take for the customer to enter their details on the card issuer’s ACS. The time the customer will spend on the ACS will depend on a number of factors. Longer wait times may occur when the customer is signing up to a 3-D Secure scheme for the first time, or recovering a forgotten password. While your system needs to allow time for the customer to return, it is entirely possible for the customer to close their browser on the card issuer's ACS and not return at all. There are no specific regulations as to how long your system must wait for the customer to be redirected from the ACS to your Term URL, but Secure Trading recommends waiting for no more than two hours.
5 Authorisation

3-D authorisations are used to seek authorisation for authenticated transactions from your acquiring bank. This is performed by submitting an AUTH XML Request to STPP and interpreting the response returned.

5.1 3-D Authorisation XML Request

This section documents how to construct an authorisation XML Request. The structure of the request is similar to that of a standard e-commerce authorisation (AUTH) request, as described in the XML Specification document. The differences are outlined in this section of the document.

5.1.1 For enrolled cards (Enrolled = ‘Y’)

For cards that are enrolled in the card issuer’s 3-D Secure scheme, you will need to submit the MD and PaRes fields (returned from the ACS in the HTTPS POST) in an AUTH XML Request to STPP.

```
request type = “AUTH” +
operation +
md
pares
```

These fields are used to inherit transaction information needed to perform the authorisation:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>operation</td>
<td></td>
<td></td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>
| md       | an   | 1024   | Y        | MD
|          |      |        |          | Must be the value returned in the md field of the THREEDQUERY XML Response, otherwise this may forfeit the liability shift. |
| pares    | an   | 65536  | Y        | PaRes
|          |      |        |          | Must be the value returned in the pares field of the HTTPS POST from the card issuer’s ACS, otherwise this may forfeit the liability shift. |
Secure Trading analyses the PaRes submitted in the AUTH XML Request to determine whether or not the cardholder was successfully authenticated on their card issuer’s ACS. We will only contact the acquiring bank to seek authorisation for the transaction if the cardholder was successfully authenticated.

5.1.1.1 Example of 3-D authorisation XML Request for enrolled cards

Please find below an example of a 3-D authorisation XML Request to be submitted to Secure Trading’s systems, for enrolled cards. Ensure you include the MD and PaRes fields returned from the ACS in your XML Request (highlighted in bold):

```xml
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
<alias>test_site12345</alias>
<request type="AUTH">
  <merchant>
    <orderreference>test.xml.threedauth</orderreference>
  </merchant>
  <operation>
    <md>UEZOVVBqeE5SRDQ4VFVSSVBtdEZjMVJpZFR0aE1EVnRhamh4YTJkJSVIwZEdUbmM5UF...
      RzFDSmZldz09
    </md>
    <pares>eJzVWFmzosgSfudXdpQ8Gt1sbkzYRhQ7KCjI/sYOsimgOL/+lp7Tp5c5t2d67tM...
      w8yv+/WqiluJXS8WyyVF EQT28qzQF/LKD8+0pK6nszk5I1f063SSFflu/vzxGHVQl8vt4Y...
    </pares>
  </operation>
</request>
</requestblock>
```

Please note that the `<md>` and `<pares>` elements typically contain values far longer than displayed in the example above and therefore have been abbreviated using ‘...’, for your convenience.

When submitting these fields, your system must submit their full values, unmodified.

Your system only needs to include the elements shown in the example above in the AUTH XML Request. All other information required to seek authorisation will be inherited from the previous 3-D query request stored on our system.

Secure Trading allows the submission of additional fields in the 3-D authorisation that have not been submitted in the 3-D query request (e.g. the customer name, if omitted in the query). For a full list of fields that can be submitted in an AUTH XML Request to STPP, please refer to the XML Specification document.
5.1.2 For not-enrolled cards (Enrolled = 'N') or unknown enrolment (Enrolled = 'U')

For cards that are NOT enrolled in the card issuer’s 3-D Secure scheme (or have unknown enrolment), you will need to submit the following fields in order to inherit transaction information needed to perform the authorisation:

```
MERCHAND
MERCHANT

AUTH Request

parent
transaction
reference

secure/trading

For cards that are NOT enrolled in the card issuer’s 3-D Secure scheme (or have unknown enrolment), you will need to submit the following fields in order to inherit transaction information needed to perform the authorisation:

request type = “AUTH” +

operation +

parent transactionreference

sitereference

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| parent
transaction reference | an   | 20     | Y        | This must be the <transactionreference> field returned in the THREEDQUERY XML Response. |
| sitereference   | an   | 50     | Y        | This must be the site reference the 3-D query was performed through.     |
5.1.2.1 Example of 3-D authorisation XML Request for not-enrolled cards (or unknown enrolment)

Please find below an example of a 3-D authorisation XML Request to be submitted to Secure Trading’s systems, for not-enrolled cards (or unknown enrolment). Ensure you include the <parenttransactionreference> and <sitereference> fields in your XML Request (highlighted in bold):

```xml
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
    <alias>test_site12345</alias>
    <request type="AUTH">
        <merchant>
            <orderreference>test.xml.threedauth</orderreference>
        </merchant>
        <operation>
            <parenttransactionreference>6-9-1188175</parenttransactionreference>
            <sitereference>test_site12345</sitereference>
        </operation>
    </request>
</requestblock>
```

Your system only needs to include the elements shown in the example above in the AUTH XML Request. All other information required to seek authorisation will be inherited from the previous 3-D query request stored on our system.

Secure Trading allows the submission of additional fields in the 3-D authorisation that have not been submitted in the 3-D query request (e.g. the customer name, if omitted in the query). For a full list of fields that can be submitted in an AUTH XML Request to STPP, please refer to the XML Specification document.
5.2 3-D Authorisation XML Response

This section documents how to interpret an authorisation XML Response. The structure of the response is similar to that of a standard e-commerce authorisation (AUTH) response, as described in the XML specification document. The differences are outlined in this section of the document.

```
response type = "AUTH"+ threedsecure
                +

    enrolled
      +

      status
      +

      cavv
      +

      eci
      +

      xid
```
### 5.2.1 `<threedsecure>`

Successful 3-D authorisation XML Responses contain a `<threedsecure>` tag, which contains a number of elements, as described in the following table:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>threedsecure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>enrolled</td>
<td>an</td>
<td>1</td>
<td>Y</td>
<td>Indicates whether or not the cardholder is enrolled in a 3-D Secure scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 'Y' - Card is enrolled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 'N' - Card is not enrolled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 'U' - Unable to determine if card is enrolled.</td>
</tr>
<tr>
<td>status</td>
<td>an</td>
<td>1</td>
<td>C*</td>
<td>Indicates whether or not the customer was authenticated on the card issuer's ACS:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 'Y' - Customer authenticated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 'N' - Customer not authenticated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 'A' - An authentication attempt occurred but could not be completed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 'U' - Unable to perform authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Only returned if card is enrolled.</td>
</tr>
<tr>
<td>cavv</td>
<td>an</td>
<td>32</td>
<td>C*</td>
<td>The unique Cardholder Authentication Verification Value (CAVV) associated with the transaction, provided by the card issuer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Only returned if card is enrolled and authenticated.</td>
</tr>
<tr>
<td>eci</td>
<td>an</td>
<td>2</td>
<td>C*</td>
<td>The ECI (E-Commerce Indicator) security level associated with the transaction.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Only returned if card is enrolled and authenticated.</td>
</tr>
<tr>
<td>xid</td>
<td>an</td>
<td>255</td>
<td>C*</td>
<td>The unique identifier for the transaction, assigned by the MPI (Merchant Plug-In) (in this case, Secure Trading).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*Only returned if card is enrolled and authenticated.</td>
</tr>
</tbody>
</table>

The above fields may be requested by a card issuer in the event of a disputed transaction and are included in the response for your reference.
5.2.2 XML Response Examples

5.2.2.1 If the card is enrolled and successfully authenticated on the ACS

The following is an example of a 3-D Secure AUTH XML Response that is returned from Secure Trading's systems for an enrolled and authenticated card. Elements needed for your system to be able to interpret the response are highlighted in **bold**:

```xml
<?xml version='1.0' encoding='utf-8'?>
<responseblock version="3.67">
  <requestreference>X995034265</requestreference>
  <response type="AUTH">
    <merchant>
      <merchantname>Test Merchant</merchantname>
      <orderreference>test.xml.threedauth</orderreference>
      <tid>00000000</tid>
      <merchantnumber>00000000</merchantnumber>
      <merchantcountryiso2a>GB</merchantcountryiso2a>
      <operatorname>test_site12345</operatorname>
    </merchant>
    <transactionreference>6-9-1188168</transactionreference>
    <timestamp>2014-06-03 09:36:00</timestamp>
    <acquirerresponsecode>00</acquirerresponsecode>
    <operation>
      <parenttransactionreference>6-9-1188157</parenttransactionreference>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
    <settlement>
      <settleduedate>2014-06-04</settleduedate>
      <settlestatus>0</settlestatus>
    </settlement>
    <billing>
      <amount currencycode="GBP">100</amount>
      <payment type="VISA">
        <issuer>SecureTrading Test Issuer1</issuer>
        <pan>4111111111111111</pan>
        <issuercountry>US</issuercountry>
      </payment>
      <dcc enabled="0"/>
    </billing>
    <authcode>TEST</authcode>
    <threedsecure>
      <cavv>Q0FWVkJNbV1ZDQVZWAQ0FWVkJNbV1Y=</cavv>
      <status>Y</status>
      <xid>NmVxNGtsTDBkSVJzcmwrSnEyMFc=</xid>
      <eci>05</eci>
      <enrolled>Y</enrolled>
    </threedsecure>
    <live>0</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
  </response>
</responseblock>
```
5.2.2.2 If the card is enrolled but NOT successfully authenticated on the ACS

The following is an example of a 3-D Secure AUTH XML Response that is returned from Secure Trading’s systems for an enrolled but un-authenticated card. Elements needed for your system to be able to interpret the response are highlighted in **bold**:

```xml
<?xml version='1.0' encoding='utf-8'?>
<responseblock version="3.67">
  <requestreference>X192311265</requestreference>
  <response type="AUTH">
    <merchant>
      <merchantname>Test Merchant</merchantname>
      <orderreference>test.xml.threedauth</orderreference>
      <id>00000000</id>
      <merchantnumber>00000000</merchantnumber>
      <merchantcountryiso2a>GB</merchantcountryiso2a>
      <operatorname>test_site12345</operatorname>
    </merchant>
    <transactionreference>23-9-2</transactionreference>
    <timestamp>2014-06-03 09:36:00</timestamp>
    <operation>
      <parenttransactionreference>23-9-1</parenttransactionreference>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
    <settlement>
      <settleduedate>2014-06-04</settleduedate>
      <settlestatus>3</settlestatus>
    </settlement>
    <billing>
      <amount currencycode="GBP">100</amount>
      <payment type="VISA">
        <issuer>SecureTrading Test Issuer1</issuer>
        <pan>4111111111111111</pan>
        <issuercountry>US</issuercountry>
      </payment>
      <dcc enabled="0"/>
    </billing>
    <threedsecure>
      <status>N</status>
      <enrolled>Y</enrolled>
    </threedsecure>
    <live>0</live>
  </response>
</responseblock>
```

Additional information:
- **status**: N (Not authenticated)
- **enrolled**: Y (Enrolled)
- **message**: Unauthenticated
- **code**: 60022

Note: Elements needed for your system to interpret the response are highlighted in **bold**.
5.2.2.3 If the card is not enrolled

The following is an example of a 3-D Secure AUTH XML Response that is returned from Secure Trading’s systems for not-enrolled card. Elements needed for your system to be able to interpret the response are highlighted in **bold**:

```xml
<?xml version='1.0' encoding='utf-8'?><responseblock version="3.67">
  <requestreference>X0e66c907</requestreference>
  <response type="AUTH">
    <merchant>
      <merchantname>Test Merchant</merchantname>
      <orderreference>test.xml.threedauth</orderreference>
      <tid>00000000</tid>
      <merchantnumber>00000000</merchantnumber>
      <merchantcountryiso2a>GB</merchantcountryiso2a>
      <operatorname>test_site12345</operatorname>
    </merchant>
    <transactionreference>23-33-4</transactionreference>
    <timestamp>2014-06-03 09:36:00</timestamp>
    <acquirerresponsecode>00</acquirerresponsecode>
    <operation>
      <parenttransactionreference>23-33-3</parenttransactionreference>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
    <acquirerresponsemessage>Approved or completed Successfully</acquirerresponsemessage>
    <settlement>
      <settleduedate>2014-06-04</settleduedate>
      <settlestatus>0</settlestatus>
    </settlement>
    <billing>
      <amount currencycode="USD">100</amount>
      <payment type="VISA">
        <pan>4111111111111102</pan>
        <issuercountry>US</issuercountry>
      </payment>
    </billing>
    <authcode>000003</authcode>
    <threedsecure>
      <enrolled>N</enrolled>
    </threedsecure>
    <live>1</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
    <security>
      <postcode>2</postcode>
      <securitycode>2</securitycode>
      <address>2</address>
    </security>
  </response>
</responseblock>
```
5.2.3 Managing Authorisation Response

Your system will need to interpret the authorisation response in order to determine if the transaction was successful. The most important field to check is the `<error><code>` element in the response.

<table>
<thead>
<tr>
<th>Error code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Cardholder was successfully authenticated on the card issuer’s ACS. Customer’s bank authorised the transaction. Funds will be transferred.</td>
</tr>
<tr>
<td>70000</td>
<td>Cardholder was successfully authenticated on the card issuer’s ACS. Customer’s bank declined the transaction. Funds will <strong>NOT</strong> be transferred.</td>
</tr>
<tr>
<td>60022</td>
<td>Cardholder was not successfully authenticated on the card issuer’s ACS. Secure Trading did not contact the acquiring bank to seek authorisation. Funds will <strong>NOT</strong> be transferred.</td>
</tr>
<tr>
<td>99999</td>
<td>An error code of ‘99999’ indicates an unknown error occurred, which requires manual inspection. We recommend contacting our Support Team for assistance (section 8.1).</td>
</tr>
<tr>
<td>Other</td>
<td>Please consult the following URL for a full list of error codes used by STPP: <a href="http://webapp.securetrading.net/errorcodes.html">http://webapp.securetrading.net/errorcodes.html</a></td>
</tr>
</tbody>
</table>

Regardless of the `<error><code>` returned in the response, Secure Trading strongly recommends you refer to the Best Practices section of the XML Specification document and configure your system to perform all of the checks outlined.
6 Using your own MPI

Secure Trading allows you to implement your own MPI to determine whether or not a customer's card is enrolled in a 3-D Secure scheme, instead of performing a 3-D query request to STPP.

6.1 Pre-requisites

## Important: If you use your own MPI, it is your responsibility to ensure your system follows the 3-D Secure specification (keeping up to date with amendments issued by Visa and/or Mastercard) with regard to VEReq/VERes messages and PARes signature verification. You must also provide Secure Trading with all valid, unaltered and verified values for each field as specified, below.

Failure to follow the specification outlined below may result in forfeiting the liability shift.

If you do not have values for specific fields listed in this section, you must **NOT** submit the fields in question in any requests to Secure Trading.

6.2 Enrolled and Authenticated Cards

After establishing the card is enrolled in the 3-D Secure scheme and the customer has been authenticated successfully, your system will need to construct an AUTH XML Request (similar to that of a standard e-commerce AUTH request described in the [XML Specification document](#)), ensuring you include all of the fields listed, below:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>threeSecure</td>
<td>an</td>
<td>32</td>
<td>C*</td>
<td>The unique Cardholder Authentication Verification Value (CAVV) associated with the transaction. *Always submit this value if it is available.</td>
</tr>
<tr>
<td>cavv</td>
<td>an</td>
<td>2</td>
<td>C*</td>
<td>The ECI (E-Commerce Indicator) security level associated with the transaction. *Always submit this value if it is available.</td>
</tr>
<tr>
<td>eci</td>
<td>an</td>
<td>255</td>
<td>C*</td>
<td>The unique identifier for the transaction, assigned by your MPI (Merchant Plug-In). *Always submit this value if it is available.</td>
</tr>
<tr>
<td>xid</td>
<td>an</td>
<td>1</td>
<td>Y</td>
<td>Indicates whether or not the customer was authenticated on the card issuer's ACS: 'Y' - Customer authenticated. 'A' - An authentication attempt occurred but could not be completed. 'U' - Unable to perform authentication.</td>
</tr>
<tr>
<td>enrolled</td>
<td>an</td>
<td>1</td>
<td>Y</td>
<td>Indicates whether or not the customer was authenticated on the card issuer's ACS: 'Y' - Customer authenticated. 'A' - An authentication attempt occurred but could not be completed. 'U' - Unable to perform authentication.</td>
</tr>
</tbody>
</table>
6.2.1 AUTH XML Request Example for Enrolled and Authenticated Cards

```
<requestblock version="3.67">
  <alias>site12345</alias>
  <request type="AUTH">
    <merchant>
      <orderid>test.xml.threedauth</orderid>
    </merchant>
    <billing>
      <postcode>TE45 6ST</postcode>
      <premise>789</premise>
      <payment type="VISA">
        <expirydate>10/2031</expirydate>
        <pan>411111000000211</pan>
        <securitycode>123</securitycode>
      </payment>
      <amount currencycode="GBP">100</amount>
    </billing>
    <operation>
      <siteref>test_site12345</siteref>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
    <threedsecure>
      <cavv>Q0FWVkNBv1ZQVZWQ0FWVkBv1Y=</cavv>
      <eci>05</eci>
      <xid>WElEWElEWElEWElEWElEWElEWElEWElEWEk=</xid>
      <enrolled>Y</enrolled>
      <status>Y</status>
    </threedsecure>
  </request>
</requestblock>
```
6.3 Not-Enrolled Cards

If the card is not enrolled in the 3-D Secure scheme, your system will need to construct an AUTH XML Request similar to that of a standard e-commerce AUTH request (see the XML Specification document), ensuring you include all of the fields listed, below:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Type</th>
<th>Length</th>
<th>Required</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>threedsecure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>enrolled</td>
<td>an</td>
<td>1</td>
<td>Y</td>
<td>Submit ‘N’ to indicate that card is not enrolled.</td>
</tr>
<tr>
<td>xid</td>
<td>an</td>
<td>255</td>
<td>C*</td>
<td>The unique identifier for the transaction, assigned by your MPI (Merchant Plug-In). *Always submit this value if it is available.</td>
</tr>
</tbody>
</table>

6.3.1 AUTH XML Request Example for Not-Enrolled Cards

```xml
<requestblock version="3.67">
  <alias>site12345</alias>
  <request type="AUTH">
    <merchant>
      <orderreference>test.xml.threedauth</orderreference>
    </merchant>
    <billing>
      <postcode>TE45 6ST</postcode>
      <premise>789</premise>
      <payment type="VISA">
        <expirydate>10/2031</expirydate>
        <pan>4111110000000211</pan>
        <securitycode>123</securitycode>
      </payment>
      <amount currencycode="GBP">100</amount>
    </billing>
    <operation>
      <sitereference:test.test_site12345</sitereference>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
    <threedsecure>
      <enrolled>N</enrolled>
      <xid>WELEWELEWELEWELEWELEWELEWELEWEk=</xid>
    </threedsecure>
  </request>
</requestblock>
```

6.4 Authorisation Response

The AUTH XML Response returned from STPP will meet the same specification as outlined in section 5.2.
7 Testing

Secure Trading recommends thoroughly testing your implementation on your test site reference before processing live transactions. This document provides examples of XML Requests and HTTPS POSTS that are required to perform 3-D Secure transactions.

By modifying these examples so that they contain your site details and include the designated test PANs (see sections 9.1 and 9.2), your system can perform tests by submitting these requests to STPP.

Although this document contains full XML examples, Secure Trading provides a downloadable folder of XML code for your convenience:

- Web Services users: http://webapp.securetrading.net/examples/WEBSERVICES.zip

Please ensure you have tested the following scenarios before going live:

- Customer’s card is not enrolled in a 3-D Secure scheme.
- Customer’s card is enrolled in a 3-D Secure scheme but not authenticated.
- Customer’s card is enrolled in a 3-D Secure scheme, authenticated but the transaction is ultimately declined by the customer’s bank.
- Customer’s card is enrolled in a 3-D Secure scheme, authenticated and the transaction is authorised by the customer’s bank.

7.1 Testing THREEDQUERY

- 3-D queries are described in section 3.
- THREEDQUERY XML Request; section 3.1.6.
- THREEDQUERY XML Response; section 3.2.3.
- If you have used a test PAN that simulates a card that is enrolled in a 3-D Secure scheme, your system will be returned an ACS URL that is a webpage hosted by Secure Trading.
7.2 Testing ACS (if card is enrolled)

Interacting with the ACS is described in section 4.

Perform an HTTPS POST to the ACS URL returned in the THREEDQUERY XML Response (see section 4 for an example).

You will be displayed our test ACS page (as shown below), where you can enter different values to test for different cases. In the textbox provided (on the right), enter the PIN from the table on the left that represents the test case you would like to process (case-sensitive).

When processing live transactions, the ACS page is hosted by the relevant card issuer.

Ensure your system is ready to handle the web browser returning from Secure Trading’s servers.

Secure Trading ACS Testing

This is a TEST ACS only
No Money will be transferred.

It will emulate a real ACS using the PINs as described.

You can force the ACS to return any type of response by entering the PIN for the card type as below.

The Status codes are as defined in the 3-D Secure Protocol.

<table>
<thead>
<tr>
<th>PIN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>sty</td>
<td>Y</td>
</tr>
<tr>
<td>stu</td>
<td>U</td>
</tr>
<tr>
<td>stn</td>
<td>N</td>
</tr>
<tr>
<td>sta</td>
<td>A</td>
</tr>
</tbody>
</table>

After the payment has been processed, the error/code and threedsecure/status values returned in the AUTH response are used to convey the final outcome.

When the threedsecure/status is “N”, indicating the customer failed authentication, the error/code “60022” will be returned.

7.3 Testing AUTH

3-D authorisations are described in section 5.

AUTH XML Request example for enrolled cards; section 5.1.1.1.

AUTH XML Request example for not-enrolled cards; section 5.1.2.1.

AUTH XML Response example for enrolled & authenticated cards; section 5.2.2.1.

AUTH XML Response example for enrolled & unauthenticated cards; section 5.2.2.2.

AUTH XML Response example for not-enrolled cards; section 5.2.2.3.
7.4 Additional Notes

When performing transactions on your test site reference:
- An amount (in base units) of 70000 will always return a declined response.
- An amount (in base units) of 60010 will always return a bank system error.
- Please ensure that within the expirydate field you set a date in the future, otherwise your system will be returned an invalid field (‘30000’) error.
8 Further Information and Support

Further Information and Support
This section provides useful information with regards to documentation and support for the Merchant's Secure Trading solution.

8.1 Secure Trading Support

Any questions regarding integration or maintenance of the system, please contact our support team using one of the following methods.

<table>
<thead>
<tr>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>+44 (0) 1248 672 050</td>
</tr>
<tr>
<td>Fax</td>
<td>+44 (0) 1248 672 099</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:support@securetrading.com">support@securetrading.com</a></td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.securetrading.com/support/support.html">http://www.securetrading.com/support/support.html</a></td>
</tr>
</tbody>
</table>

8.2 Secure Trading Sales

If you do not have an account with Secure Trading, please contact our Sales team and they will inform you of the benefits of a Secure Trading account.

<table>
<thead>
<tr>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>0800 028 9151</td>
</tr>
<tr>
<td>Telephone (Int'l)</td>
<td>+44 (0) 1248 672 070</td>
</tr>
<tr>
<td>Fax</td>
<td>+44 (0) 1248 672 079</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:sales@securetrading.com">sales@securetrading.com</a></td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.securetrading.com">http://www.securetrading.com</a></td>
</tr>
</tbody>
</table>

8.3 Useful Documents

The documents listed below should be read in conjunction with this document:

- **STPP STAPI User Guide** – This document outlines how to install the STAPI java client for processing XML Requests and Responses through STPP.
- **STPP Web Services User Guide** – This document describes how to process XML Requests and Responses through Secure Trading’s Web Services solution.
- **STPP XML Specification** – This document details the XML structure of authorisations and refunds submitted through STPP.
- **STPP Transaction Query** – This document details how to perform TRANSACTIONQUERY XML Requests to STPP.

Any other document regarding STPP can be found on Secure Trading’s website (http://www.securetrading.com). Alternatively, please contact our support team as outlined above.

8.4 Frequently Asked Questions

Please visit the FAQ section on our website (http://www.securetrading.com/support/faq).
9 Appendix

9.1 PANs to test authorisation

The following are test card details, and will not return the expected responses in a live environment. Use these to simulate authorisations with cards that are either enrolled or not enrolled in the card issuer’s 3-D Secure scheme:

<table>
<thead>
<tr>
<th>Card type</th>
<th>Enrolled ‘Y’</th>
<th>Enrolled ‘N’</th>
<th>Enrolled ‘U’</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAESTRO¹</td>
<td>5000000000000611</td>
<td>500000000000421</td>
<td>500000000000801</td>
</tr>
<tr>
<td>MAESTRO²</td>
<td>6759000000000711</td>
<td>675900000000521</td>
<td>675900000000901</td>
</tr>
<tr>
<td>MASTERCARD</td>
<td>5100000000000511</td>
<td>510000000000321</td>
<td>510000000000701</td>
</tr>
<tr>
<td>MASTERCARDDEBIT</td>
<td>2221000000000611</td>
<td>2221000000000991</td>
<td>2221000000000801</td>
</tr>
<tr>
<td>VPAY</td>
<td>4370000000000111</td>
<td>4370000000000921</td>
<td>4370000000002307</td>
</tr>
<tr>
<td>VISA</td>
<td>4111110000000211</td>
<td>4111110000000021</td>
<td>4111110000000401</td>
</tr>
<tr>
<td>DELTA³</td>
<td>40062600000002473</td>
<td>40062600000002481</td>
<td>40062600000002408</td>
</tr>
<tr>
<td>ELECTRON</td>
<td>4245190000000311</td>
<td>4245190000000121</td>
<td>4245190000000501</td>
</tr>
<tr>
<td>PURCHASING</td>
<td>4484000000000411</td>
<td>4484000000000221</td>
<td>4484000000000601</td>
</tr>
</tbody>
</table>

¹ PAN issued outside of UK  
² PAN issued in UK  
³ aka Visa Debit

9.2 PANs to test decline

The following are test card details, and will not return the expected responses in a live environment. Use these to simulate declining transactions:

<table>
<thead>
<tr>
<th>Card type</th>
<th>Decline</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAESTRO</td>
<td>5000000000000512</td>
</tr>
<tr>
<td>MASTERCARD</td>
<td>510000000000421</td>
</tr>
<tr>
<td>MASTERCARDDEBIT</td>
<td>222100000000082</td>
</tr>
<tr>
<td>VPAY</td>
<td>4370000000000112</td>
</tr>
<tr>
<td>VISA</td>
<td>4111110000000112</td>
</tr>
<tr>
<td>DELTA⁴</td>
<td>431072000000042</td>
</tr>
<tr>
<td>ELECTRON</td>
<td>4245190000000212</td>
</tr>
<tr>
<td>PURCHASING</td>
<td>4484000000000312</td>
</tr>
</tbody>
</table>

⁴ aka Visa Debit
9.3 Additional Requests

3-D Secure can be used in conjunction with other additional request types offered by Secure Trading. The 3-D query must **always** be performed **immediately before the authorisation**. When adding additional requests to a 3-D Secure and AUTH implementation, the additional request(s) must never be performed in-between the THREEDQUERY XML Request and the AUTH XML Request.

E.g. For merchants using Protect Plus, the RISKDEC XML Request must be either performed **before the THREEDQUERY XML Request** or **after the AUTH XML Request**, but never in-between. (Refer to the Protect Plus document for further information on Protect Plus).

Any other additional requests that are performed before the AUTH XML Request must always be performed before the THREEDQUERY XML Request.