

ST Xpay 3-D Secure Specification

Version 3.51

Copyright

© SecureTrading 2011. All rights reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system or transmitted in any form or by any means whether electronic, mechanical or otherwise without the prior written permission of SecureTrading Ltd.

Disclaimer

This document is for informational purposes only. SecureTrading make no warranties, express or implied, through the distribution of this document. No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by SecureTrading, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

SecureTrading reserves the right to revise the content without obligation to notify any person of such changes.

Document revised on 31 March 2011.

Contents

1	Introduction.....	4
1.1	3-D Secure process definition	4
1.2	Benefits of 3-D Secure	5
1.3	3-D Secure ST Xpay and Xpay4 process	6
2	ST3DCardQuery.....	7
2.1	ST3DCardQuery Request	7
2.1.1	XML Specification	7
2.1.1.1	<TermUrl>	8
2.1.1.2	<MerchantName>	8
2.1.1.3	<Accept>	8
2.1.1.4	<UserAgent>	8
2.1.2	XML Example	8
2.2	ST3DCardQuery response.....	9
2.2.1	XML Specification	9
2.2.1.1	<Result>	10
2.2.1.2	<Enrolled>.....	10
2.2.1.3	<Html>	10
2.2.2	Customising Redirect Html.....	10
2.2.2.1	<AcsUrl>	11
2.2.2.2	<MD>	11
2.2.2.3	<PaReq>	11
2.2.2.4	<TermUrl>.....	11
2.2.3	XML example.....	11
3	ST3DAuth.....	13
3.1	ST3D Auth request.....	13
3.1.1	XML specification	13
3.1.1.1	<Enrolled>.....	13
3.1.1.2	<PaRes>.....	13
3.1.1.3	<MD>	13
3.1.1.4	<ParentTransactionReference>	14
3.1.2	XML example.....	14
3.2	ST3D Auth response.....	15
3.2.1	XML specification	15
3.2.2	XML example.....	15
4	Testing	16
5	Switch/Maestro Debit Cards.....	16
6	Branding	17
7	Further information	18
7.1	Support.....	18
7.2	Further Reading.....	18

1 Introduction

This document describes the additional functionality available to ST Xpay and Xpay4 users regarding the processing of 3-D Secure requests via the ST Xpay or Xpay4 client. It defines the XML specification for requests using both the ST Xpay and ST Xpay4 APIs. In most cases the XML is identical for each version. Where there are differences the specification will state how Xpay and Xpay4 differ.

This document must be read in conjunction with the ST XML Specification, available on the SecureTrading web site. For document locations, please refer to the [Further Reading](#) section of this document.

1.1 3-D Secure process definition

Performing a 3-D Secure payment is split up into two distinct processes.

Firstly the customer submits their card details for verification of enrolment in the 3-D Secure scheme. This is achieved by processing a Card Query request. A Card Query request submits information to a directory server hosted by a card issuer (e.g. Visa). If a card is in the 3-D Secure scheme the Card Query response will contain html that must be relayed to the customer. This html redirects the customer to a log-in screen enabling them to validate their identity through an Access Control Server (ACS) hosted by a card issuer.

In addition to customer card details a Card Query request will contain a redirect URL (TermUrl) enabling the customer to be redirected from the ACS back to the merchants site to finalise the authentication and perform the actual authorisation.

The second part of the process involves the merchant submitting an authorisation request with payment and additional 3-D Secure validation information. The additional information required is obtained from the data that the ACS redirects to the merchant, details of which are highlighted in this document.

1.2 Benefits of 3-D Secure

Benefits of the 3-D Secure process include the enhanced security available when performing a 3-D Secure transaction and the shift of liability in the event of fraudulent transactions. If a 3-D Secure transaction is completed and has been determined to be fraudulent then the credit liability is usually shifted from the merchant and onto the card issuer.

In most 3-D Secure cases the merchant will not receive any notification of a chargeback if the transaction is disputed by the cardholder. This is a major benefit in reducing lost revenue due to fraudulent transactions. Please note however, that 3-D Secure is not a 100% guarantee that no chargebacks will be incurred. There are some restrictions for each scheme although these cases should not occur very often.

SecureTrading believe the liability shift to be as follows:

Brand	Enrolled	Status	Liability
Visa	U		Merchant*
Visa	N		Card Issuer**
Visa	Y	Y	Card Issuer**
Visa	Y	N	Merchant***
Visa	Y	A	Card Issuer**
Visa	Y	U	Merchant
MasterCard	U		Card Issuer**
MasterCard	N		Card Issuer**
MasterCard	Y	Y	Card Issuer**
MasterCard	Y	N	Merchant***
MasterCard	Y	A	Card Issuer**
MasterCard	Y	U	Card Issuer**

*** Important note:** If the brand is Visa and the enrolled or status is returned as a “U” (Unknown) this means that the merchant is **not** covered by the 3-D Secure scheme. In this case the merchant is still liable for any fraudulent transactions.

**** Important note:** There are some cases where the liability is not covered by the Card Issuer; for example non-European commercial cards under both brands. For more information please contact your acquirer.

***** Important note:** In this case it is strongly recommended that the transaction does not proceed. This means the password entered did not match.

You should apply the same fraud detection/prevention measures to 3-D Secure transactions as you do to normal transactions.

The additional security benefits and liability shifts of 3-D Secure transactions are currently only supported by cards within the Visa and MasterCard brands. Any other issued cards (e.g. Amex) submitted as a Card Query request will respond with a result 2. They can only be authorised using standard authorisation methods.

To participate in the 3-D Secure scheme please contact support at support@securetrading.com.

1.3 3-D Secure ST Xpay and Xpay4 process

ST Xpay and Xpay4 facilitate the processing of 3-D Secure transactions via additional ST Xpay and Xpay4 request types:

“ST3DCARDQUERY”
“ST3DAUTH”

The “ST3DCARDQUERY” request is used to determine whether the customer’s card is enrolled in the 3-D Secure scheme.

An “ST3DCARDQUERY” request submits information to a directory server. If the card is in the 3-D Secure scheme then the “ST3DCARDQUERY” response will contain the html required by the customer to finalise the enrolment validation, via an ACS.

As it is required by 3-D Secure to submit authentication information as part of the “ST3DAUTH” request, the ACS responds with this information. The information is sent to the merchant via a redirect to a TermUrl.

The “ST3DAUTH” request is used to send an authorisation request to SecureTrading. An “ST3DAUTH” requires the same information as a standard ST Xpay or Xpay4 “AUTH” request in addition to authentication information obtained during the “ST3DCARDQUERY” process.

Both requests and their corresponding responses adhere to the standard ST Xpay and Xpay4 XML syntax as defined in the ST XML Specification document. This document highlights the additional fields required when processing 3-D Secure requests and the 3-D Secure fields returned in a response.

2 ST3DCardQuery

A "ST3DCARDQUERY" request is the process used to determine if a credit card is in the 3-D Secure scheme. The following section details the additional XML required to process a "ST3DCARDQUERY" request and explains the information returned in the subsequent response.

2.1 ST3DCardQuery Request

2.1.1 XML Specification

To process a 3-D Secure card query request an "ST3DCARDQUERY" Request type must be submitted.

```
<Request Type="ST3DCARDQUERY">
  <Operation></Operation>
  <CustomerInfo></CustomerInfo>
  <PaymentMethod></PaymentMethod>
  <Order></Order>
</Request>
```

The <Operation> element contains the following tags all of which are required.

```
<Operation>
  <Amount>Int</Amount>
  <Currency>String</Currency>
  <SiteReference>String</SiteReference>
  <TermUrl>String</TermUrl>
  <MerchantName>String</MerchantName>
</Operation>
```

Within the <CustomerInfo> element the following tags are required.

```
<CustomerInfo>
  <Accept>String</Accept>
  <UserAgent>String</UserAgent>
</CustomerInfo>
```

The <PaymentMethod> element contains a single sub-element called <CreditCard> which is required.

```
<PaymentMethod>
  <CreditCard></CreditCard>
</PaymentMethod>
```

Within the <CreditCard> the following tags can be submitted.

```
<CreditCard>
  <Type>String</Type>
  <Number>Int</Number>
  <Issue>Int</Issue>
  <StartDate>String</StartDate>
  <ExpiryDate>String</ExpiryDate>
</CreditCard>
```

Note all but <Issue> and <StartDate> are required.

For a detailed explanation of the <PaymentMethod> element, its sub-elements and tags, the <Order> element and its tags, as well as the <Amount>, <Currency>, <SiteReference> tags please refer to the ST XML Specification document.

2.1.1.1 <TermUrl>

The <TermUrl> tag will contain the location of the merchant's script that an ACS will redirect a customer to post information to after the customer has performed their identity check via an ACS. It should fully comply with the 3-D Secure specification. In particular, some issuer ACS systems will reject a TermUrl which is too long or contains characters such as a pipeline (|).

2.1.1.2 <MerchantName>

The <MerchantName> is a mandatory field and must contain your merchant name according to the 3-D Secure specification. It has a maximum length of 25 characters.

Note: This information will be displayed to the customer when they provide their additional security information. Care must be taken to ensure that the same information is submitted as defined on the merchant's web site.

2.1.1.3 <Accept>

The <Accept> is a mandatory field and must contain the exact content of the HTTP accept-header field as received from the cardholder's request. This is required if the cardholder's user agent supplies it, otherwise you may forfeit the liability shift. If no information was available then a blank tag must be sent, e.g. <Accept></Accept>

2.1.1.4 <UserAgent>

The <UserAgent> is a mandatory field and must contain the exact content of the HTTP user-agent header field as received from the cardholder's request. This is required if the cardholder's user agent supplies it, otherwise you may forfeit the liability shift. If no information was available then a blank tag must be sent, e.g. <UserAgent></UserAgent>

2.1.2 XML Example

Following is an example of a 3-D Secure card query request. For Xpay4 an XML header specifying the version and character encoding is required. Please refer to the XML request section within the ST XML Specification document referenced in [Further Reading](#) for more details.

```
<?xml version="1.0" encoding="utf-8"?>
<RequestBlock Version="3.51">
  <Request Type="ST3DCARDQUERY">
    <Operation>
      <Amount>5000</Amount>
      <Currency>GBP</Currency>
      <SiteReference>site1234</SiteReference>
      <TermUrl>https://merchantSite.net/3dauth.cgi</TermUrl>
      <MerchantName>25 character field</MerchantName>
    </Operation>
    <CustomerInfo>
      <Accept>Accept headers</Accept>
      <UserAgent>user agent</UserAgent>
    </CustomerInfo>
    <PaymentMethod>
      <CreditCard>
        <Type>VISA</Type>
        <Number>4111111111111160</Number>
        <Issue></Issue>
        <StartDate></StartDate>
        <ExpiryDate>02/08</ExpiryDate>
      </CreditCard>
    </PaymentMethod>
  </Request>
</RequestBlock>
```

```

    <Order>
      <OrderReference>Order0001</OrderReference>
      <OrderInformation>This is a test order</OrderInformation>
    </Order>
  </Request>
  <Certificate>
  -----BEGIN CERTIFICATE-----
MIIGUTCCBg+gAwIBAgICAQMwCwYHKOZIZjgEAwUAMIG/MQswCQYDVQQGEwJVSzEP
MA0GA1UECBMTG9uZG9uMQswCQYDVQQHEwJTVDEWMBQGA1UEChMNU2VjdXJlVHJh
ZGluZzEuMCwGA1UECzMlVGZvdCBNZXJjaGFudCBDZlZlJ0aWZpY2F0aW9uIEF1dGhv
SPEeso/HNlkY8DXrEXixAhRcJrEC3JnDXLRDZc32MciHvISP9Q==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
TWhG9Qn9kJ+h15rJBvbQtNvFMBuLlIXEVOxZboteE+2lW7iYz5gF7HWUPgjm+RTM
j6D5a16AuWU0/uqL6VVe6POgBorSFeWd18RnQLfAinVkeu8UkWBs1Y4j5ICFGRC
YaJAnR5AJ4xXUK3CHVbLEBkW
-----END RSA PRIVATE KEY-----
</Certificate>
<!--NOTE for ST Xpay4 the Certificate tag should just contain your certificate alias-->
</RequestBlock>

```

2.2 ST3DCardQuery response

2.2.1 XML Specification

The “ST3DCARDQUERY” response will contain information detailing the enrolment status of the cardholder in the scheme. Depending on the result of the “ST3DCARDQUERY” certain XML fields may not be returned.

As defined in the ST XML Specification document the <Result> tag will be returned in all cases. These fields will contain the result of processing the XML request on the SecureTrading system rather than the outcome of a cardholder’s enrolment in the 3-D Secure scheme.

Note that the <Message> tag may contain a message from the SecureTrading Merchant Plugin (MPI) defined by the 3-D Secure specification stating you should perform a normal authorisation request. This does not mean an e-commerce “AUTH” request. The table below shows the correct course of action.

The following table represents a guide to the action a merchant should take to fulfil the 3-D Secure criteria and assist in the reduction of any liability issues that may arise. A detailed breakdown of the response fields follows.

<Result>	<Enrolled>	Auth Request Type
0	N/A	Retry “ST3DCARDQUERY” or submit normal “AUTH” request.
1	Y	Must perform “ST3DAUTH” request.
1	N	Must perform “ST3DAUTH” request.
1	U	Must perform “ST3DAUTH” request.
2	N/A	Must perform normal “AUTH” request.

The following additional fields may be present in the <OperationResponse> depending on the result of performing the request:

```

<OperationResponse>
  <Enrolled>Char</Enrolled>
  <Html>String</Html>
  <TermUrl>String</TermUrl>
  <AcsUrl>String</AcsUrl>
  <PaReq>String</PaReq>
  <MD>String</MD>
</OperationResponse>

```

For a definition of the <TransactionReference> tag, please refer to the ST XML Specification document..

2.2.1.1 <Result>

The <Result> tag will contain one of the following values.

Result	Reason	Comment
0	An error was encountered during processing	Consult the <Message> tag and depending on the error reason the card query can be re-attempted or a normal "AUTH" can be performed. See Note 1.
1	The request was successfully processed	A 3-D Secure Authorisation ("ST3DAUTH") must be submitted.
2	The request was successfully processed but the 3-D Secure process cannot be continued	The 3-D Secure process cannot proceed. An "AUTH" can be processed if required. See Note 1.

Note 1: If a normal authorisation is processed then the liability shift associated with 3-D Secure will not apply. Maestro International cards cannot be processed as a normal AUTH request.

In the case of an error, additional information explaining the response will be included in the <Message> tag.

2.2.1.2 <Enrolled>

The <Enrolled> tag will contain the results of performing the "ST3DCARDQUERY" request with the acquiring bank. The values returned will be one of the following.

Y	The cardholder is enrolled in the scheme and a 3-D Secure authentication can be performed
N	The cardholder is not in the 3-D Secure scheme
U	The directory server was unable to determine if the cardholder is enrolled in the 3-D Secure scheme

2.2.1.3 <Html>

In the case of receiving an <Enrolled> of Y, this field will contain the html that may be used to redirect the cardholder's browser in order for them to continue with the 3-D Secure validation by connecting to an access control server.

This can be achieved by sending your normal server headers to the client immediately followed by the contents of the <Html> tag.

2.2.2 Customising Redirect Html

If you wish to customise the redirect html instead of using the contents of 2.2.1.3 <Html>, then the following tags will be needed. Note you will need to ensure that your Html conforms to the 3D Secure specification – it must contain both Content-Type and Content-Length headers, the cardholders browser must POST the form to the ACS, the action must be initiated though the card holders browser and must be performed with as little action on the part of the card holder as possible. If JavaScript is used for redirection there must also be a fall-back for environments that do not support JavaScript. (see 3-D Secure: Functional Requirements – Merchant Server Plug-in for further details:

http://www.visaeurope.com/documents/vbv/verifiedbyvisa_merchantdeploymentbestpractices.pdf.

2.2.2.1 <AcsUrl>

This is the url of the ACS it should be used as the location of the redirect.

2.2.2.2 <MD>

The <MD> is a unique reference generated according to the 3-D Secure specification (currently up to 1024 bytes in base64 format). It will be returned to the merchant in the case of receiving an <Enrolled> of Y. This can be used by the merchant to tie up a response obtained from an ACS after the customer's authentication process. See section 3.1.1.3 for further details.

If you are making your own customised redirect page instead of using the <Html> provided then this field MUST be included in that html, as a hidden field.

2.2.2.3 <PaReq>

The <PaReq> contains purchase transaction details upon which ACS authentication decisions are based.

If you are making your own customised redirect page instead of using the <Html> provided then this field MUST be included in that html, as a hidden field. The length of the PaReq is not explicitly defined by the 3-D Secure specification. We recommend allowing at least 4096 bytes for this field in any variables/storage systems.

2.2.2.4 <TermUrl>

In the case of receiving an <Enrolled> of Y, this field will contain the TermUrl that was sent in the request. See section 2.1.1.1 <TermUrl>

If you are making your own customised redirect page instead of using the <Html> provided then this field MUST be included in that html as a hidden field.

2.2.3 XML example

The following is an example of a successful "ST3DCARDQUERY" response indicated by the result of 1.

```

<ResponseBlock Live="TRUE" Version="3.51">
  <Response Type="ST3DCARDQUERY">
    <OperationResponse>
      <TransactionReference>100-9-2321</TransactionReference>
      <Result>1</Result>
      <Enrolled>Y</Enrolled>
      <MD>LFKHDSPLFIHPOSEHFIKEHFEDDES</MD>
      <PaReq>KGRwMQpTJ0V4cG9uZW50JwpwMgpJMgpzUydjdXJyZW5jeScKc
GUGdGltZScKcDQ3CnNTJ01lcklEJwpwNDgKZzE3CnMu</PaReq>
      <TermUrl>https://merchantSite.net/3dauth.cgi</TermUrl>
      <AcUrl>https://anIssuer.net/acs.cgi</AcUrl>
      <Html>&lt;!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN">
&lt;/HTML>&lt;/HEAD>&lt;TITLE>Redirecting...&lt;/TITLE>&lt;META http-
equiv='Content-Type' content='tex
t/html; charset=utf-8'>&lt;/HEAD>
&lt;BODY onload="setTimeout('document.form.submit()', '500')">
&lt;H2>If you are not redirected automatically please click to continue&lt;/H2>
&lt;FORM name='form' id='form' METHOD='POST'
ACTION='https://anIssuer.net/acs.cgi'>
&lt;P>&lt;INPUT type='hidden' name='PaReq'
value='KGRwMQpTJ0V4cG9uZW50JwpwMgpJMgpzUydjdXJyZW5jeScKc
GUGdGltZScKcDQ3CnNTJ01lcklEJwpwNDgKZzE3CnMu'>
&lt;INPUT type='hidden' name='TermUrl'
value='https://merchantSite.net/3dauth.cgi'>
&lt;INPUT type='hidden' name='MD' value='LFKHDSPLFIHPOSEHFIKEHFEDDES'>
&lt;INPUT TYPE='submit' VALUE='          Continue          ' SIZE='30'>
&lt;/P>&lt;/FORM>&lt;/BODY>&lt;/HTML></Html>
    </OperationResponse>
  </Response>
</ResponseBlock>

```

3 ST3DAuth

The following section details the information required to perform an "ST3DAUTH" request.

3.1 ST3D Auth request

A "ST3DAUTH" request contains the same request data as an "AUTH" request (as described in the ST XML Specification document) with the addition of 3-D Secure related information. The following sections describe the extra fields. It is important that this request type is used for cards which are covered by the 3-D Secure scheme. However, the use of this request type will not guarantee that any liability is shifted from the merchant.

Note the request type must be set to "ST3DAUTH", e.g.

```
<Request Type="ST3DAUTH">
```

3.1.1 XML specification

In addition to the standard authorisation request the inclusion of a <ThreeDSecure> element is required. This element must be included in the <PaymentMethod> element of the XML, e.g.

```
<PaymentMethod>
  <CreditCard></CreditCard>
  <ThreeDSecure></ThreeDSecure>
</PaymentMethod>
```

Within the <ThreeDSecure> element there are three tags.

```
<ThreeDSecure>
  <Enrolled>Char</Enrolled>
  <PaRes>String</PaRes>
  <MD>String</MD>
</ThreeDSecure>
```

3.1.1.1 <Enrolled>

The <Enrolled> is a mandatory field. The value returned in the "ST3DCARDQUERY" response should be submitted. See section 2.2.1.2 for details.

3.1.1.2 <PaRes>

The <PaRes> tag is a mandatory field. Data required in the tag will have been returned from the ACS to the customer's browser and then re-directed to the merchant script defined in the "ST3DCARDQUERY" <TermUrl> tag. This will only be available if the <Enrolled> response was a Y when performing a "ST3DCARDQUERY". The value of the PaRes may vary depending on the card issuer, but conforms to the 3-D Secure specification (in particular the value is base64 encoded). For any other <Enrolled> response the tag should be submitted empty, i.e. <PaRes></PaRes>. The length of the PaRes is not explicitly defined by the 3-D Secure specification. We recommend allowing at least 65536 bytes for this field in any variables/storage systems.

3.1.1.3 <MD>

The <MD> tag is a mandatory field. Data required in the tag will have been returned from the ACS to the customer's browser and then re-directed to the merchant script defined in the "ST3DCARDQUERY" <TermUrl> tag. This will only be available if the <Enrolled> response was a Y when performing a "ST3DCARDQUERY". The content of the <MD> tag returned from the ACS will be

the same as the <MD> returned in the "ST3DCARDQUERY" response. For any other <Enrolled> response the tag should be submitted empty, i.e. <MD></MD>.

3.1.1.4 <ParentTransactionReference>

The <ParentTransactionReference> is a mandatory field and must contain the reference returned in the "ST3DCARDQUERY" <TransactionReference> tag.

Note as defined in the ST XML Specification document the <ParentTransactionReference> tag is located within the <CreditCard> element.

3.1.2 XML example

The following example is an ST3DAUTH request after completing a successful "ST3DCARDQUERY" indicated by an <Enrolled> of Y and the presence of a <PaRes> and <MD>. For Xpay4 an XML header specifying the version and character encoding is required. Please refer to the XML request section within the ST XML Specification document referenced in [Further Reading](#) for more details.

```
<?xml version="1.0" encoding="utf-8"?>
<RequestBlock Version="3.51">
  <Request Type="ST3DAUTH">
    <Operation>
      <Amount>5000</Amount>
      <Currency>GBP</Currency>
      <SiteReference>site1234</SiteReference>
      <SettlementDay>1</SettlementDay>
    </Operation>
    <CustomerInfo>
      <Postal>
        <Name>
          <FirstName>Joe</FirstName>
          <LastName>Bloggs</LastName>
        </Name>
        <Street>A Street</Street>
        <CountryCode>UK</CountryCode>
      </Postal>
    </CustomerInfo>
    <PaymentMethod>
      <CreditCard>
        <Type>VISA</Type>
        <Number>4111111111111160</Number>
        <StartDate></StartDate>
        <ExpiryDate>02/08</ExpiryDate>
        <SecurityCode></SecurityCode>
        <ParentTransactionReference>100-9-2321</ParentTransactionReference>
      </CreditCard>
      <ThreeDSecure>
        <Enrolled>Y</Enrolled>
        <PaRes>ABJASDKA+SDKAJ/SGDSAD</PaRes>
        <MD>LFKH/DSPLFIHPO+SEHFKEHFEDES</MD>
      </ThreeDSecure>
    </PaymentMethod>
    <Order>
      <OrderReference>Order0001</OrderReference>
      <OrderInformation>This is a test order</OrderInformation>
    </Order>
  </Request>
  <Certificate>
    -----BEGIN CERTIFICATE-----
    MIIGUTCCBg+gAwIBAgICAQMwCwYHKOZIZjgEAwUAMIG/MQswCQYDVQQGEwJVSzEP
    SPEeso/HNlkY8DXrEXixAhRcJrEC3JnDXLRDZc32MciHvISP9Q==
    -----END CERTIFICATE-----
    -----BEGIN RSA PRIVATE KEY-----
```

```
j6D5a16AuWU0/uqL6VVe6POgBorSFeWd18RnQLfAinVkeu8UkWQBS1Y4j5ICFGRC
-----END RSA PRIVATE KEY-----
</Certificate>
```

<!--NOTE for ST Xpay4 the Certificate tag should just contain your certificate alias-->

```
</RequestBlock>
```

3.2 ST3D Auth response

Upon processing an ST3DAUTH request, an XML response will be returned to the merchant.

3.2.1 XML specification

The returned XML when performing an ST3DAUTH will be the same as that of a normal authorisation request with the only difference being the value of the TYPE attribute in the <Response> element. Please refer to the Auth Response section of the ST XML Specification document.

3.2.2 XML example

```
<ResponseBlock Live="FALSE" Version="3.51">
  <Response Type="ST3DAUTH">
    <OperationResponse>
      <TransactionReference>232-9-1162</TransactionReference>
      <AuthCode>AUTH CODE:TEST</AuthCode>
      <Result>1</Result>
      <SettleStatus>0</SettleStatus>
      <SecurityResponseSecurityCode>1</SecurityResponseSecurityCode>
      <SecurityResponsePostcode>2</SecurityResponsePostcode>
      <SecurityResponseAddress>4</SecurityResponseAddress>
      <TransactionCompletedTimestamp>2003-12-05
10:10:24</TransactionCompletedTimestamp>
      <TransactionVerifier>AsA/QW9r3wujUakAhVW4dtXMJDZx</TransactionVerifier>
    </OperationResponse>
    <Order>
      <OrderReference>Order0001</OrderReference>
      <OrderInformation>This is a test order</OrderInformation>
    </Order>
    <ThreeDSecure>
      <Status>Y</Status>
      <XID>ODI5NDY4NS4wODI5NDUxMjgyNTI=</XID>
      <Enrolled>Y</Enrolled>
      <ECI>05</ECI>
      <CAVV>0123456789012345678901234567</CAVV>
    </ThreeDSecure>
  </Response>
</ResponseBlock>
```

4 Testing

In order to ensure your 3-D Secure implementation fulfils the specification we highly recommend you complete all of the following test cases:

Card number ¹	Username ²	Expected Results in your viewscreens ³			
		Type	Result	Enrolled	Status
Visa not in scheme	n/a	ST3DAUTH	1	N	n/a
Visa in scheme	sty	ST3DAUTH	1	Y	Y
Visa in scheme	stu	ST3DAUTH	1	Y	U
Visa in scheme	sta	ST3DAUTH	1	Y	A
Visa in scheme	stn	ST3DAUTH	2	Y	N
Visa unknown	n/a	ST3DAUTH	1	U	n/a
MasterCard in scheme	sty	ST3DAUTH	1	Y	Y
Maestro with/without issue	sty	ST3DAUTH	1	Y	Y
MasterCard not in scheme	n/a	ST3DAUTH	1	N	n/a
AMEX	n/a	AUTH	1	n/a	n/a

NB. The **Result** column in this table also refers to the <Result> in the final XML response from ST Xpay or Xpay4, not the <Result> in the ST3DCARDQUERY response.

5 Switch/Maestro Debit Cards

Now that MasterCard have re-branded Switch cards to Maestro, SecureTrading now classify any Switch card that has not been re-branded, as a Maestro debit card and you are required to submit “Maestro” in place of “Switch” for the card type when processing an authorisation.

A secondary change that MasterCard is enforcing is that all Maestro cards must use MasterCard SecureCode, current SecureTrading merchants will continue to be able to process Switch/Maestro cards as normal authorisations but will be required to update their transaction processing so that all Maestro debit cards are processed using MasterCard SecureCode.

Most acquirers supporting 3-D Secure can process Maestro cards through MasterCard SecureCode although you may be required to have additional merchant account numbers and/or agreements.

IMPORTANT: By processing Maestro debit cards after July 1st as normal authorisations, you may incur a fine from MasterCard.

Please contact SecureTrading support for more information.

¹ Please refer to the SecureTrading Testing Document for valid test credit card numbers

² Enter this value on the SecureTrading test ACS page

³ After completing the transactions please ensure these values have appeared in your My-ST viewscreens

6 Branding

Both Visa and MasterCard have specific requirements for the branding of their respective 3-D Secure schemes. Before going live you should obtain a copy of the guidelines for each brand you have registered with and ensure any requirements are met.

This includes (but is not limited to):

- Scheme logo(s): Including size, colour, placement
- Scheme link(s): Including help pages for new customers
- Scheme text: How and when to write the brand names
- Maestro branding and logo use

Your acquirer may provide you with the guidelines. If not, please contact SecureTrading support.

7 Further information

This section contains contact information and further reading on SecureTrading products and services.

7.1 Support

SecureTrading provides support for its software and the operation of its payment service. If you require technical support, first ensure that you have read and understood all relevant documentation.

If the problem persists, please email support@securetrading.com, quoting your SecureTrading site reference and concisely stating the nature of your problem.

To help us help you, please include the original XML string sent and any error messages that are returned by the ST Xpay API verbatim. Care should be taken NOT to include sensitive payment details such as credit cards.

SecureTrading additional contact details:

Phone: 01248 672 050

Fax: 01248 672 099

7.2 Further Reading

For further information please refer to the following documents:

In the ST Xpay documents (<http://www.securetrading.com/xpay.html>) section of the SecureTrading website:

- SecureTrading XML Specification document

In the General Setup Guides (<http://www.securetrading.com/general-setup-guides.html>) section of the SecureTrading website:

- Going live guide

Bundled with the ST Xpay distribution:

- ST Xpay read me: readme.txt

3-D Secure: Functional Requirements – Merchant Server Plug-in

- http://www.visaeurope.com/documents/vbv/verifiedbyvisa_merchantdeploymentbestpractices.pdf

Other useful links:

- <http://www.international.visa.com/fb/paytech/secure/main.jsp>
- <http://www.mastercardmerchant.com/securecode>
- <http://www.mastercardbrandcenter.com>