Protect Plus

This document details the XML required to process Protect Plus Risk Decision requests via Secure Trading.

Version: 1.14 (a)
Published: 1 August 2017

Table of Contents

1 Introduction

This document explains the XML Requests and Responses involved when implementing Protect Plus using STAPI / Web Services interfaces.

We recommend you read the **Protect Plus Guide** before continuing.
This provides an overview of Protect Plus.
All Secure Trading documents can be found on our website.

Please note that Protect Plus does not guarantee against fraud. You should consider all data regarding a transaction before accepting the payment.

This document should be read in conjunction with the **XML Specification**.

1.1 Process

Your server submits a RISKDEC XML Request to Secure Trading including the customer's details. The Protect Plus system analyses the details using a rule-based system, including:

- The industry's largest negative database.
- Neural-based fraud assessments.
- Tumbling or Swapping, where there is an unusual usage pattern in the card number, expiration date or customer details associated with a transaction.

Please note that by default, when your account is configured to use Secure Trading Protect Plus, a pre-defined set of rules from the Secure Trading Protect Plus profile will be used. For information on using your own profile and any other questions, please contact the Secure Trading Sales team (see section 7.2).

Secure Trading returns a RISKDEC XML Response with the following codes:

- **ACCEPT** - The details are not deemed suspicious.
- **DENY -** The details are suspicious and a transaction should not be performed.
- **CHALLENGE** - Further investigation is recommended.
- **NOSCORE** – When a parent authorisation has been declined by the acquiring bank.

1.1.1 Supported Payment Types

It is possible to perform Risk Decision assessments for all payment types supported by Secure Trading.

1.1.2 3-D Secure Support

Protect Plus can be used in conjunction with 3D Secure. For further information, please refer to section 6.1.

1.2 About the RISKDEC Request Type and other Secure Trading Request Types

Risk Decision (RISKDEC) is the XML Request type for submissions to the Protect Plus System. RISKDEC Requests are used with other Requests to STPP, either by preceding / following these other Requests in sequence, or by being combined into a single multi-process request.

This document contains icons representing Authorisation (AUTH) and RISKDEC Requests, which are often submitted together. These icons are described, below.

		
A single rectangle represents a single XML Request submission.	A green “A” represents an AUTH Request.	A red “R” represents a RISKDEC Request.

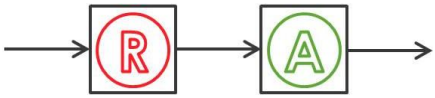
1.3 Sequence of RISKDEC and AUTH Requests

You can process a Risk Decision call where:

1.3.1 A Risk Decision Request is submitted on its own

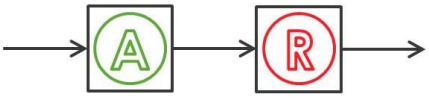
Please refer to section **2**.

1.3.2 Authorisation Request inherits details of a previous Risk Decision



Follow the specification outlined in section **2** to submit the initial Risk Decision Request, and when submitting an associated Authorisation Request, include the transaction reference of the parent Risk Decision in the **`<parenttransactionreference>`** field.

1.3.3 A Risk Decision Request inherits details of a previous Authorisation attempt



Please refer to section **3**.

Risk Decision Requests can reference authorised or declined transactions.

1.3.4 A Risk Decision and an Authorisation are combined in a single XML Request

OR

Please refer to section **4**.

The order in which the Requests are positioned within the combined XML Request dictates the order in which they are processed.

1.4 Managing Authorisations based on Risk Decision Responses

Based on the result of the Risk Decision, you can decide whether to automatically proceed with the authorisation or not. Based on the Risk Decision Response, authorisations have the following process flow by default (configured by Support upon sign-up):

1. Risk Decision returns an **ACCEPT** response, continue with the authorisation.
2. Risk Decision returns a **CHALLENGE** or **DENY** response, process the authorisation and suspend the transaction allowing for further investigation.

Please note the default process flow can be customised. For example, you could choose not to process the authorisation if the Risk Decision returns a **DENY**. For more information, contact Secure Trading Support (see **7.1 Secure Trading** Support).

1.5 Following Authorisations with Risk Decision Requests

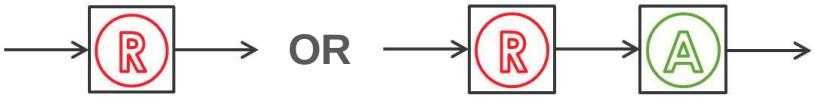
By referencing Authorisation Requests in Risk Decision Requests, you are providing the Protect Plus system with additional information, such as results of address verification checks (**AVS**), security code checks (**CVV2**) and 3-D Secure. The results of these checks would not be returned until after an authorisation is processed.

It is important to also perform Risk Decision Requests with details of declined authorisation attempts, as well as successful authorisations, as this information can be used to improve the accuracy of Risk Decision responses. For example, consider the following scenario:

> *A customer has 3 consecutive declined transactions, all on different cards, and then processes a successful authorisation.*
>
> If the Protect Plus system is only aware of the successful authorisation, it may be deemed less suspicious than if the system had details of 3 previous declined attempts for that customer.

Please note that by processing an Authorisation first, then a Risk Decision Request, the Risk Decision Response will not affect the Authorisation as described in section **1.4**.

2 RISKDEC XML Specification

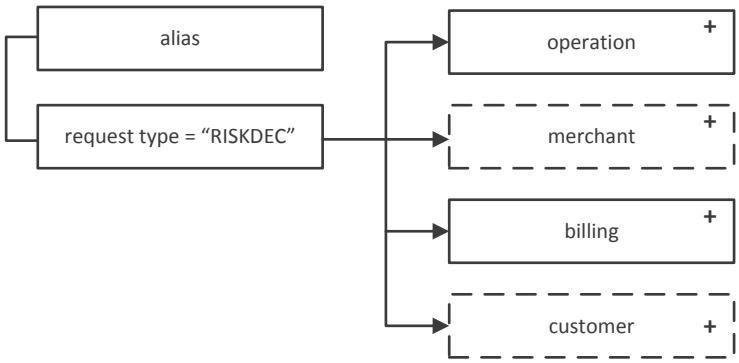


This section of the document outlines the specification of a standalone Risk Decision (RISKDEC) XML Request to be submitted to Secure Trading and the XML Response returned.

The details submitted within this request can be inherited in future requests, such as Authorisations, by including the transaction reference returned in the RISKDEC XML Response in the **<parenttransactionreference>** of the subsequent XML Request.

2.1 RISKDEC XML Request

This section of the document outlines a standalone Risk Decision (RISKDEC) XML Request.

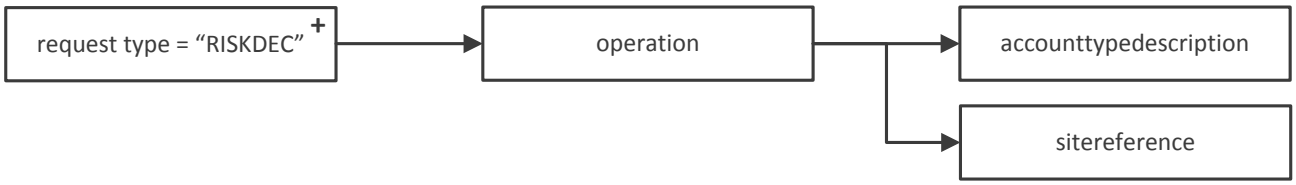


Please note although some of the fields below are marked as non-mandatory, Secure Trading recommend submitting as much data as possible as this will assist in the decision making process.

2.1.1 <request type="RISKDEC">

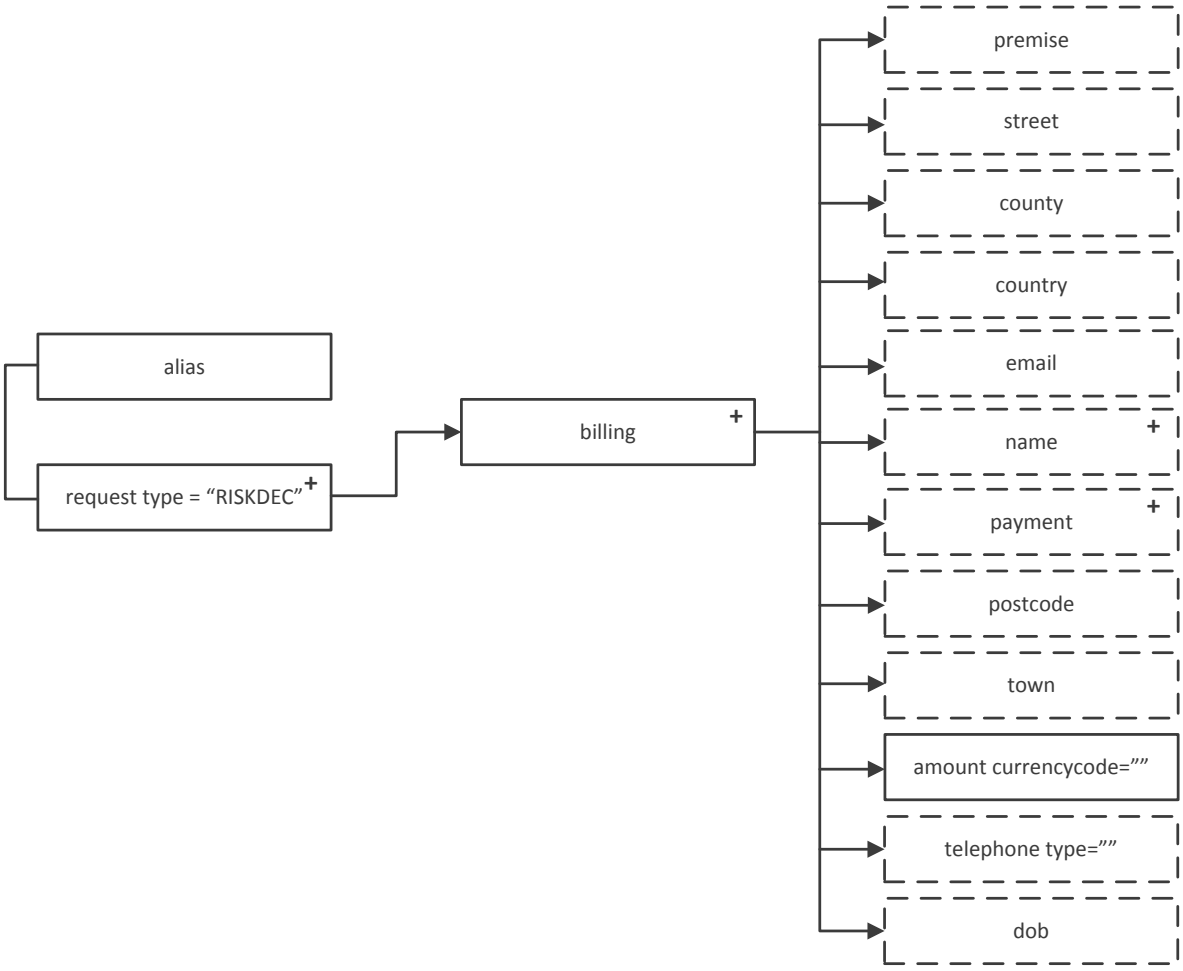
Tag	Type	Length	Required	Comment
`request type= "RISKDEC"`	an	7	Y	Must be set as "**RISKDEC"**.

2.1.2 <operation>



Tag		Type	Length	Required	Comment
operation				Y	
	sitereference	an	20	Y	Secure Trading site reference that uniquely identifies the Merchant's account.
	accounttype description	an	20	Y	Set as "**FRAUDCONTROL**".

2.1.3 <billing>



Please note the following XML parameter tables assume the customer is paying with a credit or debit card. For non-card payment types, other relevant <**payment**> fields should be used instead of **<pan>** and **<expirydate>**.

For more information, please refer to the documentation for the preferred payment type at http://www.securetrading.com/support.

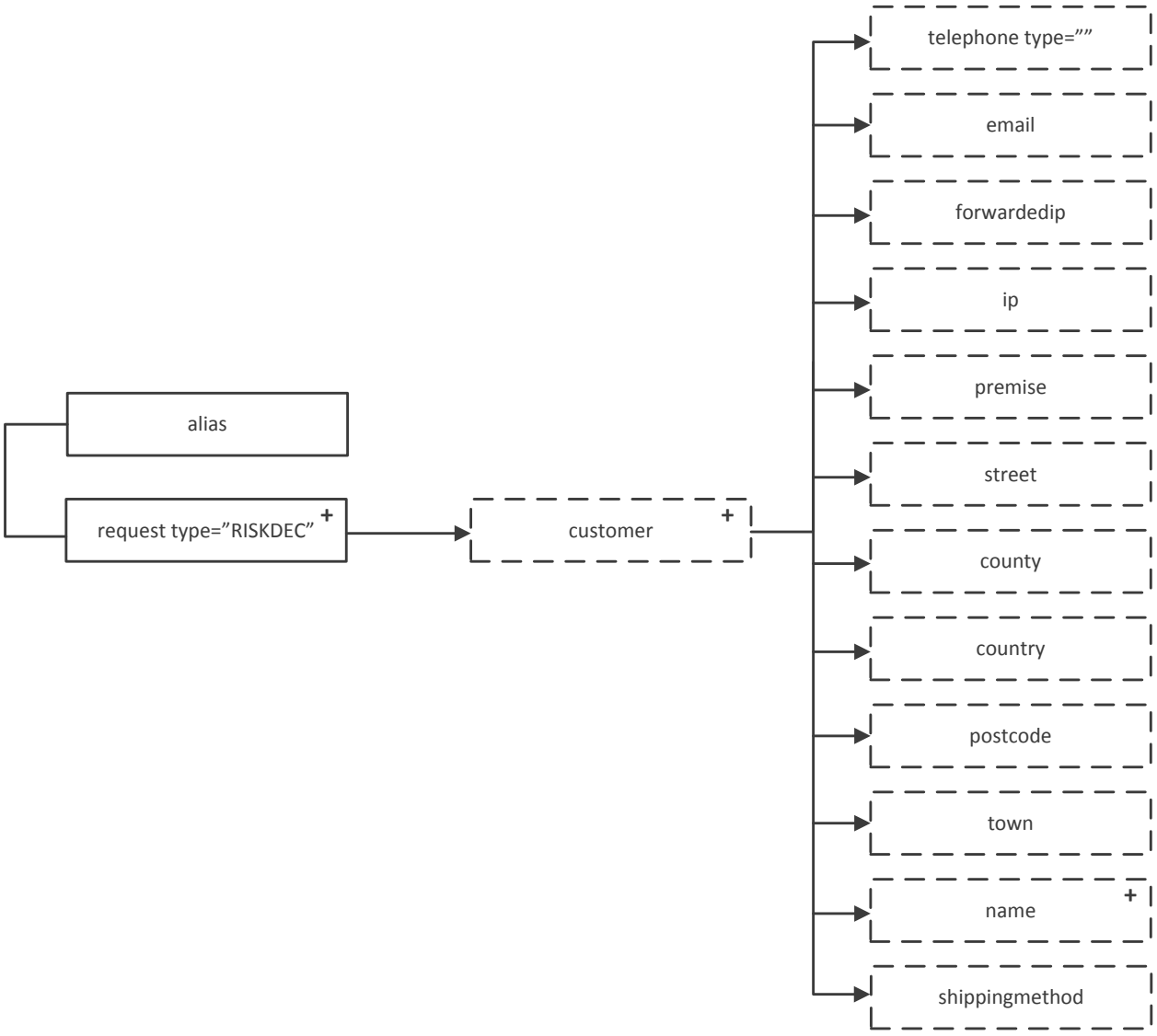
Tag	Type	Length	Required	Comment
billing			Y	
payment type=""	an	20	N	The customer's card type.
expiry date	an	7	N	This must be in the format MM/YYYY.
pan	n	12-19	N	Credit card number printed on the front of the customer's card.
name			N	
prefix	an	25	N	The name prefix of the billing details.
first	an	25	N	The first name of the billing details.
middle	an	25	N	The middle name(s) of the billing details.
last	an	25	N	The last name of the billing details.
suffix	an	25	N	The name suffix of the billing details.
premise	an	25	N	The billing address premise (house name or number).
street	an	127	N	The billing address street name.
town	an	127	N	The town of the billing address.
county	an	127	N	The county of the billing address.
postcode	an	25	N	The postcode of the billing address. This must be a valid US state code if the country is US.
country	an	3	N	The billing country ISO code. For a list of countries, see http://webapp.securetrading.net/countrycodes.html
email	an	255	N	The billing email address. Maximum length of 255 (maximum of 64 characters before the"@" symbol).

telephone type=""	an	1	N	The type of telephone number. The options available are:
				// H = Home
				// M = Mobile
				// W = Work

telephone	n	20	N	The billing telephone number. Valid characters:
				// Numbers 0-9
				// Spaces
				// Special characters: + - ( )

amount currency code=""	an	3	Y	The currency the transaction will be processed in. For a list of currencies, see http://webapp.securetrading.net/currencycodes.html
amount	an	15	Y	The transaction amount in base units with no commas or decimal points, so £10 would be 1000
dob	an	10	N	The customer's date of birth. Must be in the format YYYY-MM-DD.

2.1.4 <customer>



Tag	Type	Length	Required	Comment
customer			N	
name			N	
prefix	an	25	N	The customer's name prefix.
first	an	25	N	The customer's first name.
middle	an	25	N	The customer's middle name(s).
last	an	25	N	The customer's surname.
suffix	an	25	N	The customer's name suffix.

telephone type=""	an	1	N	The type of telephone number. The options available are:
				// H = Home
				// M = Mobile
				// W = Work

telephone	n	20	N	The customer's telephone number. Valid characters:
				// Numbers 0-9
				// Spaces
				// Special characters: + - ( )

email	an	255	N	The Customer's email address.
forwardedip	an	39	N	The Customer's forwarded IP address, as provided by a proxy server if available
ip	an	39	N	The IP of the Customer.
premise	an	25	N	The customer's house name or no.
street	an	127	N	The street name.
town	an	127	N	The town of the customer's address.
county	an	127	N	The county of the Customer address. This must be a valid US state code if the country is US.
country	an	3	N	The customer country ISO code. For a list of country codes, see http://webapp.securetrading.net/countrycodes.html
postcode	an	25	N	The postcode of the customer's address. This must be a valid US state code if the country is US.
shipping method	an	1	N	If applicable, the Customer's shipping method. Can be one of the following: **C** = Low Cost **D** = Designated by Customer **I** = International **M** = Military **N** = Next Day/Overnight **O** = Other **P** = Store Pickup **T** = 2 day Service **W** = 3 day Service

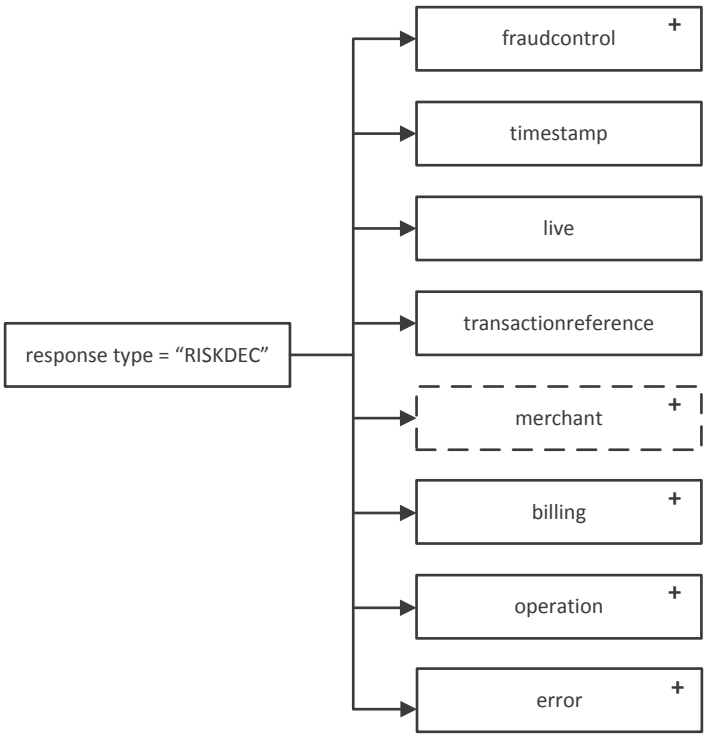
2.1.5 RISKDEC XML Request Example

The following XML example is to process a standalone Risk Decision Request:

```
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
  <alias>site12345</alias>
  <request type="RISKDEC">
    <merchant>
      <orderreference>FRAUDCONTROL</orderreference>
    </merchant>
    <billing>
      <name>
        <middle>joe</middle>
        <prefix>Dr</prefix>
        <last>bloggs</last>
        <suffix>Jr.</suffix>
        <first>fred</first>
      </name>
      <premise>789</premise>
      <street>Test Street</street>
      <town>Bangor</town>
      <county>Gwynedd</county>
      <country>GB</country>
      <postcode>TE45 6ST</postcode>
      <email>fred.bloggs@example.com</email>
      <telephone type="M">0777777777</telephone>
      <amount currencycode="GBP">1011</amount>
      <dob>1983-12-08</dob>
      <payment type="VISA">
        <expirydate>10/2031</expirydate>
        <pan>4000000000000051</pan>
      </payment>
    </billing>
    <customer>
      <name>
        <middle>Mary</middle>
        <prefix>Miss</prefix>
        <last>Smith</last>
        <first>Joanne</first>
      </name>
      <premise>111</premise>
      <street>Second Street</street>
      <town>Bangor</town>
      <county>Gwynedd</county>
      <country>GB</country>
      <postcode>CU888ST</postcode>
      <ip>1.2.3.4</ip>
      <forwardedip>1.2.3.4</forwardedip>
      <email>fred.bloggs@example.com</email>
      <telephone type="H">1111111111</telephone>
      <shippingmethod>T</shippingmethod>
    </customer>
    <operation>
      <accounttypedescription>FRAUDCONTROL</accounttypedescription>
      <sitereference>site12345</sitereference>
    </operation>
  </request>
</requestblock>
```

2.2 RISKDEC XML Response

This section of the document outlines the RISKDEC XML Response, which is returned from Secure Trading following a successful RISKDEC XML Request.

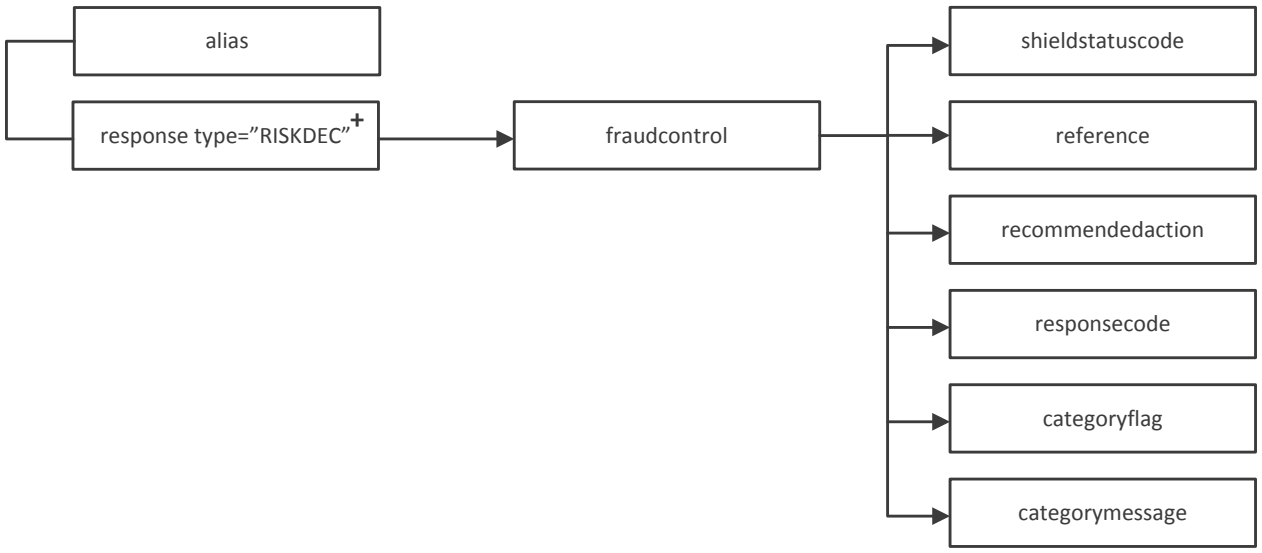


2.2.1 <response type="RISKDEC">

Tag	Type	Length	Required	Comment
`response type= "RISKDEC"`	an	7	Y	This will be "**RISKDEC"**.

2.2.2 <fraudcontrol>

The results of the Risk Decision checks are in the <**fraudcontrol**> tags.



Tag	Type	Length	Required	Comment
fraudcontrol			Y	
shieldstatus code	an	10	Y	One of the following: **ACCEPT** = The details are not deemed suspicious. **CHALLENGE** = Further investigation is recommended. **DENY** = The details are suspicious and a transaction should not be performed. **NOSCORE** = Returned when a parent Authorisation Request has been declined.
reference	an	255	Y	The reference of the Risk Decision check.
recommended action	an	1	Y	One of the following: **C** = Continue with the transaction. **S** = Stop transaction.
responsecode	n	4	Y	Response code relating to the Risk Decision check. For more information, see section **2.2.2.1<responsecode>**.
categoryflag	an	255	C	Reference used to identify a condition that was met in order to return the **DENY** or **CHALLENGE** shield status code.
category message	an	No max limit	C	Condition that was met in order to return the **DENY** or **CHALLENGE** shield status code.

If the `<shieldstatuscode>` returned in the `<fraudcontrol>` tags is DENY, the details are deemed suspicious and it is recommended that you do not proceed with the payment.

Please note that the `categoryflag` and `categorymessage` elements will only be returned if you are using a Secure Trading Protect Plus profile.

2.2.2.1 <responsecode>

The value returned in the <**responsecode**> tags maps to the following descriptions.

<responsecode>	Description
0100	Accept.
0150	An attribute associated with an Order matched a pre-configured 'Always Accept' rule.
0200	The card number appeared in a bank or card association negative file database.
0250	An attribute associated with an Order matched a pre-configured 'Always Deny' rule.
0300	A combination of customized rules and neural-based fraud assessments has determined the card usage is suspicious and possibly fraudulent.
0330	A customized rule in the ReDShield Velocity Rules Engine returned a CHALLENGE response.
0400	A combination of customized rules and neural-based fraud assessments has determined the card usage is suspicious and possibly fraudulent and the card number appeared in a Retail Decisions card database.
0500	A combination of customized rules and neural-based fraud assessments has determined the card usage is questionable and possibly fraudulent. The overall ReDShield assessment has fallen into a 'gray area', as defined by Retail Decisions and the Client.
0600	The card number associated with the Order was found in a Retail Decisions card database.
0700	Velocity or Rules Threshold Violation. An attribute associated with an Order has exceeded a preconfigured rules threshold.
0800	Tumbling and/or Swapping Pattern Detected. The ReDShield Tumbling and Swapping engine detected an unusual usage pattern in the card number, expiration date, or customer email address associated with a transaction.
1300	The transaction has been flagged in a screening database.
901	An internal ReDShield error has occurred. Contact Secure Trading Support.
902	The format of a particular field is invalid or a required input field is missing. Please check your transaction string.

2.2.3 <operation>

Tag	Type	Length	Required	Comment
operation			Y	
accounttype description	an	12	Y	Will return “**FRAUDCONTROL**”.

2.2.4 RISKDEC XML Response Example – "ACCEPT"

The following XML example is of an "**ACCEPT**" Risk Decision Response. By including the transaction reference of this Risk Decision in a future Authorisation Request, the previously submitted details can be inherited.

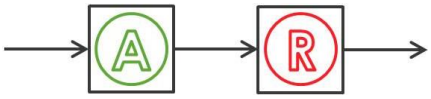
```
<?xml version="1.0" encoding="utf-8"?>
<responseblock version="3.67">
  <requestreference>X336659733</requestreference>
  <response type="RISKDEC">
    <merchant>
      <orderreference> FRAUDCONTROL</orderreference>
      <operatorname>site12345</operatorname>
    </merchant>
    <transactionreference>18-65-2</transactionreference>
    <billing>
      <payment type="VISA">
        <pan>400000######0051</pan>
      </payment>
    </billing>
    <timestamp>2012-06-21 13:32:43</timestamp>
    <fraudcontrol>
      <shieldstatuscode>ACCEPT</shieldstatuscode>
      <reference>TEST</reference>
      <recommendedaction>C</recommendedaction>
      <responsecode>0100</responsecode>
    </fraudcontrol>
    <live>0</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
    <operation>
      <accounttypedescription>FRAUDCONTROL</accounttypedescription>
    </operation>
  </response>
</responseblock>
```

2.2.5 RISKDEC XML Response Example – "DENY"

The following XML example is of a "**DENY**" Risk Decision Response. The structure of the XML is the same as with an "**ACCEPT**" RISKDEC XML Response, as shown in **section 2.2.4**. The differences in the field contents returned are shown in the following XML example:

```
<?xml version="1.0" encoding="utf-8"?>
<responseblock version="3.67">
  <requestreference>X117013583</requestreference>
  <response type="RISKDEC">
…
    <fraudcontrol>
      <categoryflag>PROBLEM2, PROBLEM3</categoryflag>
      <categorymessage>A problem2,A problem 3</categorymessage>
      <shieldstatuscode>DENY</shieldstatuscode>
      <reference>4</reference>
      <recommendedaction>S</recommendedaction>
      <responsecode>0400</responsecode>
    </fraudcontrol>
…
  </response>
</responseblock>
```

3 Risk Decision with Authorisation as a parent transaction reference



This section of the document outlines the specification of a Risk Decision (**RISKDEC**) XML Request that inherits from a previously submitted Authorisation Request and the XML Response that Secure Trading will return.

3.1 RISKDEC with AUTH Parent XML Request

A RISKDEC XML Request, which inherits details from a parent Authorisation transaction, will have the same structure as a normal RISKDEC XML Request, as described in section **2.1 RISKDEC XML Request**, except for the following differences:

Please note that when using this solution, it is required that you submit the RISKDEC Request, even if the parent Authorisation Request has been declined. All declined card details are stored by the Protect Plus system, in order to aid the prevention of future fraudulent transactions.

3.1.1 <operation>

You must include the transaction reference of the parent Authorisation transaction:

Tag	Type	Length	Required	Comment
operation			Y	
parent transaction reference	an	25	Y	Transaction reference of the parent transaction.

3.1.2 <billing>

The date of birth associated with the paying customer cannot be inherited from the parent Authorisation transaction, and can only be submitted in the RISKDEC Request:

Tag	Type	Length	Required	Comment
billing			N	
dob	an	10	N	The customer's date of birth. Must be in the format YYYY-MM-DD.

3.1.3 <customer>

The customer's chosen shipping method cannot be inherited from the parent Authorisation transaction, and can only be submitted in the RISKDEC Request:

Tag	Type	Length	Required	Comment
customer			N	
shippingmethod	an	1	N	If applicable, the Customer's shipping method. Can be one of the following: **C** = Low Cost **D** = Designated by Customer **I** = International **M** = Military **N** = Next Day/Overnight **O** = Other **P** = Store Pickup **T** = 2 day Service **W** = 3 day Service

3.1.4 RISKDEC with AUTH Parent XML Request Example

The following XML example is to process an RISKDEC Request which refers to a parent Authorisation transaction:

```
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
  <alias>site12345</alias>
  <request type="RISKDEC">
    <merchant>
      <orderreference>FRAUDCONTROL</orderreference>
    </merchant>
    <billing>
      <dob>1983-12-08</dob>
    </billing>
    <customer>
      <shippingmethod>T</shippingmethod>
    </customer>
    <operation>
   <parenttransactionreference>13-2-81001</parenttransactionreference>
      <accounttypedescription>FRAUDCONTROL</accounttypedescription>
      <sitereference>site12345</sitereference>
    </operation>
  </request>
</requestblock>
```

3.2 RISKDEC with AUTH Parent XML Response

The XML Response for Risk Decision inheriting from a parent Authorisation has the same structure as a standalone Risk Decision Response, apart from the following differences:

3.2.1 <operation>

Tag	Type	Length	Required	Comment
operation			Y	
parent transaction reference	an	25	Y	Transaction reference of the authorisation.

3.2.2 <fraudcontrol>

The values returned in the <**fraudcontrol**> tags will be the same as described in section **2.2.2 <fraudcontrol>**, unless the parent transaction reference was declined.

Tag	Type	Length	Required	Comment
fraudcontrol			Y	
shield status code	an	10	Y	"**NOSCORE**" = If the parent transaction reference was declined, then this value will always be "**NOSCORE**".

4 Combined RISKDEC and AUTH in a single XML Request

Risk Decision (RISKDEC) and Authorisation (AUTH) Requests can be submitted within a single XML Request.

If the RISKDEC is positioned first in the XML Request (before the AUTH), this request will be processed first, followed by the AUTH.

The outcome of the Risk Decision can be used to automatically suspend suspicious Authorisations and allow you to investigate the details before deciding to proceed with or to cancel the transaction.

Please refer to section **4.1** (below) for a full XML specification.

If the AUTH is positioned first in the XML Request (before the RISKDEC), this request is processed first, followed by the RISKDEC Request.

The outcome of the AVS (Address Verification System) and CVV2 (security code) checks performed by the acquiring bank can be used in the Risk Decision to give a better indicator of whether the transaction is legitimate.

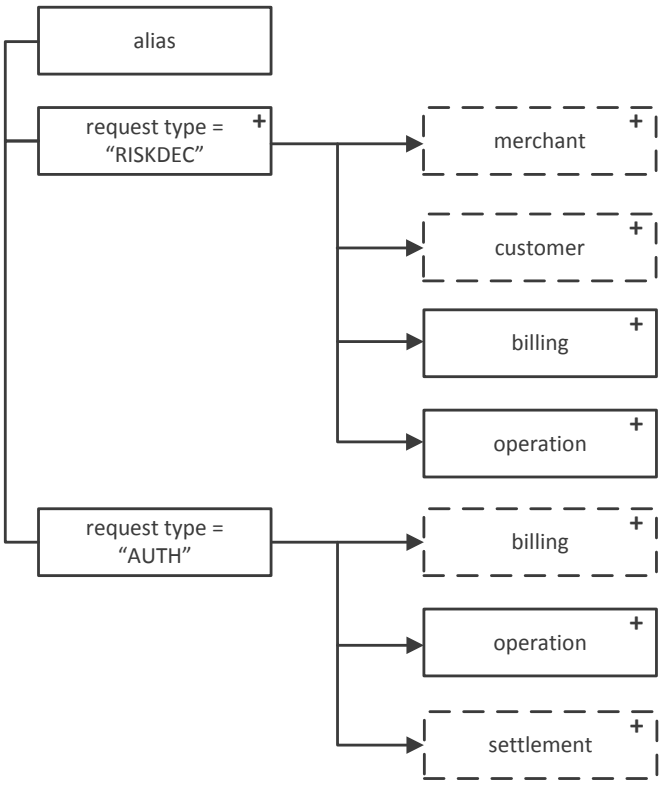
Please refer to section 4.2 for a full XML specification.

4.1 Risk Decision followed by an Authorisation

By default, the result of the Risk Decision will affect the outcome of the subsequent Authorisation Request.

Please refer to section **1.4** for more information.

4.1.1 RISKDEC and AUTH XML Request Overview



The fields that must be included within the AUTH tags as they cannot be inherited or are different to the values in the RISKDEC Request are outlined below:

4.1.1.1 <billing>

Tag	Type	Length	Required	Comment
billing			Y	
payment			Y	
securitycode	an	4	N	Security Code printed on the back of the customer's card.

4.1.1.2 <operation>

Tag	Type	Length	Required	Comment
operation			Y	
accounttype description	an	4	Y	**ECOM** – Ecommerce transaction**.** **MOTO –** Mail Order Telephone Order transaction.

4.1.2 RISKDEC and AUTH XML Request Example

The following is an XML example of a RISKDEC and AUTH Request submitted in the same request block:

```
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
  <alias>site12345</alias>
  <request type="RISKDEC">
    <merchant>
      <orderreference>riskdec_with_auth</orderreference>
    </merchant>
```

```
    <customer>
      <name>
        <middle>Mary</middle>
        <prefix>Miss</prefix>
        <last>Smith</last>
        <first>Joanne</first>
      </name>
      <premise>111</premise>
      <street>Second Street</street>
      <town>Bangor</town>
      <county>Gwynedd</county>
      <country>GB</country>
      <postcode>CU888ST</postcode>
      <telephone type="H">1111111111</telephone>
      <shippingmethod>N</shippingmethod>
      <ip>1.2.3.4</ip>
      <forwardedip>1.2.3.4</forwardedip>
      <email>fred.bloggs@example.com</email>
    </customer>
    <billing>
      <name>
        <middle>joe</middle>
        <prefix>Dr</prefix>
        <last>bloggs</last>
        <suffix>Jr.</suffix>
        <first>fred</first>
      </name>
      <premise>789</premise>
      <street>Test Street</street>
      <town>Bangor</town>
      <county>Gwynedd</county>
      <postcode>TE45 6ST</postcode>
      <country>GB</country>
      <email>fred.bloggs@example.com</email>
      <telephone type="M">0777777777</telephone>
      <amount currencycode="GBP">1011</amount>
      <dob>1983-12-08</dob>
      <payment type="VISA">
        <expirydate>10/2031</expirydate>
        <pan>4000000000000051</pan>
      </payment>
    </billing>
    <operation>
      <accounttypedescription>FRAUDCONTROL</accounttypedescription>
      <sitereference>site12345</sitereference>
    </operation>
  </request>
  <request type="AUTH">
    <billing>
      <payment>
        <securitycode>123</securitycode>
      </payment>
    </billing>
    <operation>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
  </request>
</requestblock>
```

4.1.3 RISKDEC and AUTH XML Response Example – "ACCEPT" Response

The XML Response will include the response for RISKDEC and AUTH. The following XML example is of a combined RISKDEC and AUTH Response, where the AUTH was processed because the RISKDEC returned an "ACCEPT" response.

More information on AUTH Requests and Responses can be found in the **STPP XML Specification** (see section **7.3 Useful Documents**).

```
<?xml version="1.0" encoding="utf-8"?>
<responseblock version="3.67">
  <requestreference>X336659733</requestreference>
  <response type="RISKDEC">
    <merchant>
      <orderreference>riskdec_with_auth</orderreference>
      <operatorname>site12345</operatorname>
    </merchant>
    <transactionreference>18-65-2</transactionreference>
    <billing>
      <payment type="VISA">
        <pan>400000######0051</pan>
      </payment>
    </billing>
    <timestamp>2012-06-21 13:32:43</timestamp>
    <fraudcontrol>
      <shieldstatuscode>ACCEPT</shieldstatuscode>
      <reference>TEST</reference>
      <recommendedaction>C</recommendedaction>
      <responsecode>0100</responsecode>
    </fraudcontrol>
    <live>0</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
    <operation>
      <accounttypedescription>FRAUDCONTROL</accounttypedescription>
    </operation>
  </response>
  <response type="AUTH">
    <merchant>
      <merchantname>Example Merchant</merchantname>
      <orderreference>riskdec_with_auth</orderreference>
      <tid>27882788</tid>
      <merchantnumber>00000000</merchantnumber>
      <merchantcountryiso2a>GB</merchantcountryiso2a>
    </merchant>
    <transactionreference>18-9-10</transactionreference>
    <security>
      <postcode>2</postcode>
      <securitycode>2</securitycode>
      <address>2</address>
    </security>
    <billing>
      <amount currencycode="GBP">1011</amount>
      <payment type="VISA">
        <issuercountry>ZZ</issuercountry>
        <pan>400000######0051</pan>
      </payment>
      <dcc enabled="0"/>
```

```
    </billing>
    <authcode>TEST</authcode>
    <timestamp>2012-06-21 13:32:43</timestamp>
    <settlement>
      <settleduedate>2012-06-21</settleduedate>
      <settlestatus>0</settlestatus>
    </settlement>
    <live>0</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
    <acquirerresponsecode>00</acquirerresponsecode>
    <operation>
      <parenttransactionreference>18-65-2</parenttransactionreference>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
  </response>
</responseblock>
```

4.1.4 RISKDEC and AUTH XML Response Example – "DENY" Response

The XML Response will include the response for RISKDEC and AUTH. The following XML example is of a combined RISKDEC and AUTH Response, where the AUTH was processed but suspended by Secure Trading because the RISKDEC returned a "DENY" response.

The structure of the XML is the same as with an "ACCEPT" RISKDEC XML Response, as shown in section **4.1.3**. The differences returned in the field contents are shown in the following XML example.

More information on AUTH Requests and Responses can be downloaded from Secure Trading's website (http://www.securetrading.com/support/stpp-xml.html).

```
<?xml version="1.0" encoding="utf-8"?>
<responseblock version="3.67">
  <requestreference>X134334505</requestreference>
  <response type="RISKDEC">
    …
    <fraudcontrol>
      <categoryflag>PROBLEM2, PROBLEM3</categoryflag>
      <categorymessage>A problem2,A problem 3</categorymessage>
      <shieldstatuscode>DENY</shieldstatuscode>
      <reference>4</reference>
      <recommendedaction>S</recommendedaction>
      <responsecode>0400</responsecode>
    </fraudcontrol>
    …
  </response>
  <response type="AUTH">
    …
    <settlement>
      <settleduedate>2012-06-22</settleduedate>
      <settlestatus>2</settlestatus>
    </settlement>
    …
  </response>
</responseblock>
```

4.2 Authorisation followed by a Risk Decision

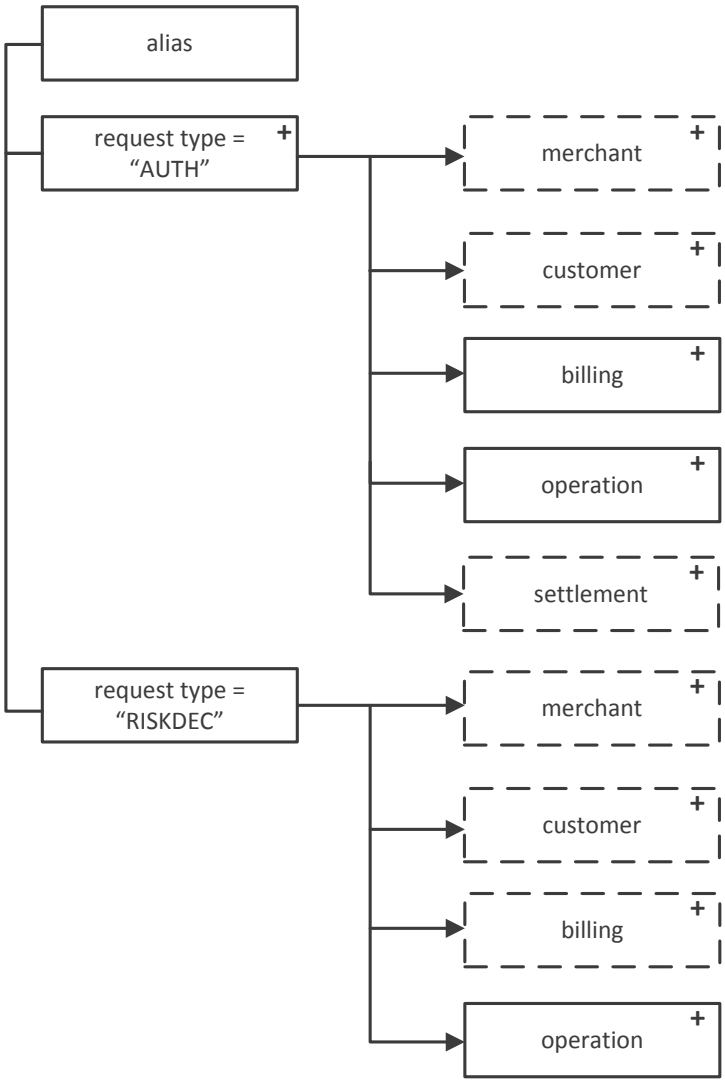
Performing the Authorisation before the Risk Decision allows the Risk Decision to take into account the results of the AVS (Address Verification System) and CVV2 (security code) checks performed by the acquiring bank on the customer's payment details.

Please see section **1.5** for further information.

Please note that by processing an Authorisation first, then a Risk Decision Request, the Risk Decision Response will not affect the outcome of the Authorisation, as in section **4.1**.

4.2.1 AUTH and RISKDEC XML Request Overview

The fields that must be included within the RISKDEC tags as they cannot be inherited from the AUTH are outlined below.



4.2.1.1 <billing>

The date of birth associated with the paying customer cannot be inherited from the parent Authorisation transaction, and can only be submitted in the RISKDEC Request:

Tag	Type	Length	Required	Comment
billing			N	
dob	an	10	N	The customer's Date of Birth. Must be in the format YYYY-MM-DD.

4.2.1.2 <customer>

The customer's chosen shipping method cannot be inherited from the parent Authorisation transaction, and can only be submitted in the RISKDEC Request:

Tag	Type	Length	Required	Comment
customer			N	
shippingmethod	an	1	N	If applicable, the Customer's shipping method. Can be one of the following: **C** = Low Cost **D** = Designated by Customer **I** = International **M** = Military

					N = Next Day/Overnight **O** = Other **P** = Store Pickup **T** = 2 day Service W = 3 day Service

4.2.2 AUTH and RISKDEC XML Request Example

The following is an XML example of an AUTH and RISKDEC Request submitted in the same request block:

```
<?xml version="1.0" encoding="utf-8"?>
<requestblock version="3.67">
  <alias>site12345</alias>
  <request type="AUTH">
    <operation>
      <sitereference>site12345</sitereference>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
    <merchant>
      <orderreference>Example AUTH</orderreference>
      <email></email>
      <name>Merchant Name</name>
    </merchant>
    <customer>
      <ip>1.2.3.4</ip>
    </customer>
    <billing>
      <email>customer.stpp@securetrading.com</email>
      <amount currencycode="GBP">1011</amount>
      <town>Bangor</town>
      <country>GB</country>
      <name>
        <first>testing</first>
      </name>
      <payment type="VISA">
        <expirydate>12/2024</expirydate>
        <pan>4111111111111111</pan>
        <securitycode>123</securitycode>
      </payment>
    </billing>
  </request>
  <request type="RISKDEC">
    <merchant>
      <orderreference>FRAUDCONTROL</orderreference>
    </merchant>
    <billing>
      <dob>1983-12-08</dob>
    </billing>
    <customer>
      <shippingmethod>T</shippingmethod>
    </customer>
    <operation>
      <accounttypedescription>FRAUDCONTROL</accounttypedescription>
      <sitereference>site12345</sitereference>
    </operation>
  </request>
</requestblock>
```

4.2.3 AUTH and RISKDEC XML Response Example – AUTH is authorised

The XML Response will include the response for AUTH and RISKDEC. The following XML example is of a combined AUTH and RISKDEC Response, where the RISKDEC returned "ACCEPT" and the Authorisation was successful.

More information on AUTH Requests and Responses can be downloaded from Secure Trading's website (http://www.securetrading.com/support/stpp-xml.html).

```
<?xml version="1.0" encoding="utf-8"?>
<responseblock version="3.67">
  <requestreference>X670186352</requestreference>
  <response type="AUTH">
    <merchant>
      <merchantname>Example Merchant</merchantname>
      <orderreference>Example AUTH</orderreference>
      <tid>27882200</tid>
      <merchantnumber>11223344</merchantnumber>
      <merchantcountryiso2a>GB</merchantcountryiso2a>
      <operatorname>site12345</operatorname>
    </merchant>
    <transactionreference>18-2-81006</transactionreference>
    <security>
      <postcode>0</postcode>
      <securitycode>2</securitycode>
      <address>0</address>
    </security>
    <billing>
      <amount currencycode="GBP">1011</amount>
      <payment type="VISA">
        <issuer>Secure Trading Test Issuer</issuer>
        <issuercountry>ZZ</issuercountry>
        <pan>411111######1111</pan>
      </payment>
      <dcc enabled="0"/>
    </billing>
    <authcode>6</authcode>
    <timestamp>2012-09-14 14:30:31</timestamp>
    <settlement>
      <settleduedate>2012-09-14</settleduedate>
      <settlestatus>0</settlestatus>
    </settlement>
    <live>1</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
    <acquirerresponsecode>00</acquirerresponsecode>
    <operation>
      <accounttypedescription>ECOM</accounttypedescription>
    </operation>
  </response>
  <response type="RISKDEC">
    <merchant>
      <orderreference>FRAUDCONTROL</orderreference>
    </merchant>
    <transactionreference>18-65-7</transactionreference>
    <billing>
      <payment type="VISA">
        <pan>411111######1111</pan>
```

```
      </payment>
    </billing>
    <timestamp>2012-09-14 14:30:31</timestamp>
    <fraudcontrol>
      <shieldstatuscode>ACCEPT</shieldstatuscode>
      <reference>5</reference>
      <recommendedaction>C</recommendedaction>
      <responsecode>0100</responsecode>
    </fraudcontrol>
    <live>1</live>
    <error>
      <message>Ok</message>
      <code>0</code>
    </error>
    <operation>
  <parenttransactionreference>18-2-81006</parenttransactionreference>
      <accounttypedescription>FRAUDCONTROL</accounttypedescription>
    </operation>
  </response>
</responseblock>
```

4.2.4 AUTH and RISKDEC XML Response Example – AUTH is declined

The XML Response will include the response for AUTH and RISKDEC. The following XML example is of a combined AUTH and RISKDEC Response, where the RISKDEC returned "NOSCORE" because the Authorisation was declined.

The structure of the XML is the same as with an authorised AUTH XML Response, as shown in section **4.2.3**. The differences in the field contents returned are shown in the following XML example.

More information on AUTH Requests and Responses can be downloaded from Secure Trading's website (http://www.securetrading.com/support/stpp-xml.html).

```
<?xml version="1.0" encoding="utf-8"?>
<responseblock version="3.67">
  <requestreference>X863091420</requestreference>
  <response type="AUTH">
    …
    <authcode>DECLINED</authcode>
    …
    <settlement>
      <settleduedate>2012-09-14</settleduedate>
      <settlestatus>3</settlestatus>
    </settlement>
    …
    <error>
      <message>Decline</message>
      <code>70000</code>
    </error>
    …
  </response>
  <response type="RISKDEC">
    …
    <fraudcontrol>
      <categoryflag>PROBLEM2,PROBLEM3</categoryflag>
      <shieldstatuscode>NOSCORE</shieldstatuscode>
      <categorymessage>A problem2,A problem3</categorymessage>
      <reference>6</reference>
      <recommendedaction>S</recommendedaction>
      <responsecode>0250</responsecode>
    </fraudcontrol>
    …
  </response>
</responseblock>
```

5 Testing

This section contains various examples of Risk Decision XML Requests. These examples can be used to test the different responses with Secure Trading's test system.

Please note the following example uses **TEST** details, and will not return the expected response in a **LIVE** environment.

5.1 Testing RISKDEC

In order to test for different RISKDEC XML Responses, please use the XML examples outlined in this document. You will need to substitute the amount submitted for those found in the following table, in order to generate the different shield status codes that can be returned in the XML Response (see section **2.2.2 <fraudcontrol>**). You will also need to use the site reference of your test account.

Base amount	Possible response codes returned	Shield status code returned
1011, **2011**, **3011**	**0100**, **0150**	**ACCEPT**
1033, **2033**, **3033**	**0300**, **0330**, **0500**	**CHALLENGE**
1044, **2044**, **3044**	**0250**, **0400**, **0600**, **0700**, **0800**, **1300**	**DENY**

Please note that shield status codes and response codes returned in XML Responses may vary when not using the amounts listed in the table, above.

Please refer to the following sections of the document for XML examples to be used when testing RISKDEC with STPP:

Type of request	Reference to XML Request	Reference to XML Response
Stand-alone RISKDEC	**Page 11**	"ACCEPT" Response on **page 15** "DENY" Response on **page 15**
RISKDEC with AUTH parent	**Page 17**	
RISKDEC and AUTH combined (RISKDEC first)	**Page 20**	"ACCEPT" Response on **page 22** "DENY" Response on **page 23**
RISKDEC and AUTH combined (AUTH first)	**Page 26**	"AUTHORISED" Response on **page 27** "DENY" Response on **page 29**

5.2 Testing Authorisation

For your reference, the following test card details can be used to test authorisation. In order to test a RISKDEC combined with an AUTH Request, please submit the examples in sections **4.1 Risk Decision followed by an Authorisation** and **4.2 Authorisation followed by a Risk Decision** , including the site reference of your Secure Trading test site.

Name of payment type	Payment type field	Authorisation	Decline
American Express	AMEX	340000000000611	340000000000512
Diners	DINERS	3000000000000111	3000000000000012
Discover	DISCOVER	6011000000000301	6011000000000202
JCB	JCB	3528000000000411	3528000000000312
Maestro	MAESTRO	5000000000000611	5000000000000512
Mastercard	MASTERCARD	5100000000000511	5100000000000412
Mastercard Debit	MASTERCARDDEBIT	5124990000000101	5124990000000002
V PAY	VPAY	4370000000000061	4370000000000012
Visa	VISA	4111110000000211	4111110000000112
Visa Debit	DELTA	4310720000000091	4310720000000042
Visa Electron	ELECTRON	4245190000000311	4245190000000212
Visa Purchasing	PURCHASING	4484000000000411	4484000000000312

For these cards, when performing tests, you need to input an expiry date that is in the future in order for the transactions to be authorised by Secure Trading's test bank.

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.

6 Additional Notes

6.1 Protect Plus with 3-D Secure

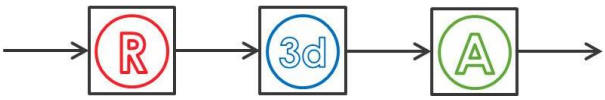
Protect Plus can be used in conjunction with 3-D Secure.

This section introduces the icon pictured left to show a 3-D query request to STPP.

6.1.1 Performing the Risk Decision BEFORE the 3-D query and authorisation

When performing the Risk Decision request **before** the 3-D query and authorisation, the result of the Risk Decision request can assist you in deciding whether or not to proceed with the transaction. Secure Trading automatically suspends transactions deemed suspicious by the Protect Plus system.

- To implement this, your system will first need to submit a Risk Decision request to STPP, as documented in section 2.1.
- After this, your system will then submit a 3-D query request, ensuring the `<transactionreference>` of the Risk Decision response is submitted in the `<parenttransactionreference>` field.
- You will need redirect the customer's browser to the ACS and perform an authorisation request (if the customer has been authenticated). This procedure is outlined in detail in the **3-D Secure XML Specification**.



6.1.2 Performing the Risk Decision AFTER the 3-D query and authorisation

When performing the Risk Decision request **after** the 3-D query and authorisation, information on whether or not the customer is enrolled in 3-D Secure (in addition to the results of the AVS and security code checks) can be used by the Protect Plus system to assist you in deciding whether or not to proceed with the transaction.

- To implement this, your system will first need to submit a 3-D query request, redirect the customer to the ACS and perform an authorisation request (if the customer has been authenticated). This procedure is outlined in detail in the **3-D Secure XML Specification**.

- After this, your system will then submit a Risk Decision request to STPP, as documented in section 2.1, but also including the **<transactionreference>** returned in the authorisation response, submitted in the **<parenttransactionreference>** field.

You must not perform a Risk Decision request between the 3-D query and the authorisation.

Further details on implementing 3-D Secure on your system can be found in the **3-D Secure XML Specification**
All Secure Trading documents can be found on our website.

7 Further Information and Support

This section provides useful information with regards to documentation and support for your Secure Trading solution.

7.1 Secure Trading Support

If you have any questions regarding integration or maintenance of the system, please contact our support team using one of the following methods:

Method	Details
Telephone	+44 (0) 1248 672 050
Fax	+44 (0) 1248 672 099
Email	support@securetrading.com
Website	http://www.securetrading.com/support/support.html

7.2 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.

Method	Details
Telephone	0800 028 9151
Telephone (Int'l)	+44 (0) 1248 672 070
Fax	+44 (0) 1248 672 079
Email	sales@securetrading.com
Website	http://www.securetrading.com

7.3 Useful Documents

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

- STPP Protect Plus Guide - This document provides a brief summary of Protect Plus.
- STAPI User Guide – This document outlines how to install the STAPI java client that can be used to process XML Requests and Responses.
- 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 structure of AUTH, REFUND and ACCOUNTCHECK XML Requests and Responses, processed through Secure Trading.
- 3-D Secure XML Specification – This document explains how to process transactions with 3D Secure using STAPI and Web Services.

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

7.4 Frequently Asked Questions

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