



## Protect Plus Guide

**Version: 1.2**

**Published: 9 May 2016**

**Table of Contents**

**1 Introduction ..... 3**

1.1 What is Protect Plus? ..... 3

1.2 How it works? ..... 3

**2 Process Overview ..... 4**

2.1 Perform Risk Decision check first - Then seek authorisation ..... 4

2.2 Seek authorisation first - then perform a Risk Decision check ..... 5

**3 Configuration..... 6**

3.1 Payment Pages ..... 6

3.2 API..... 6

**4 Viewing the Results in MyST ..... 7**

**5 Additional Notes..... 9**

5.1 Supported Payment Types..... 9

5.2 3-D Secure Support ..... 9

5.3 Testing..... 9

**6 Further Information and Support ..... 10**

6.1 Secure Trading Support ..... 10

6.2 Secure Trading Sales..... 10

6.3 Useful Documents..... 10

6.4 Frequently Asked Questions ..... 10

**7 Appendix ..... 11**

7.1 Response Codes..... 11

## 1 Introduction

### 1.1 What is Protect Plus?

Secure Trading Protect Plus adds an additional request called Risk Decision to the standard Secure Trading Protect feature set.

This document explains how Risk Decisions work and how they can be implemented on your account.

### 1.2 How it works?

A Risk Decision analyses the customer's billing, delivery and payment details using a rule-based system to detect suspicious patterns in user activity. The system will assist you in making a decision on whether to process a customer's transaction based on the perceived level of risk. Checks performed include:

- // 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 Risk Decision does not guarantee against fraud. You should consider all data regarding a transaction before accepting the payment.

The Risk Decision system will analyse these details and return the following results:

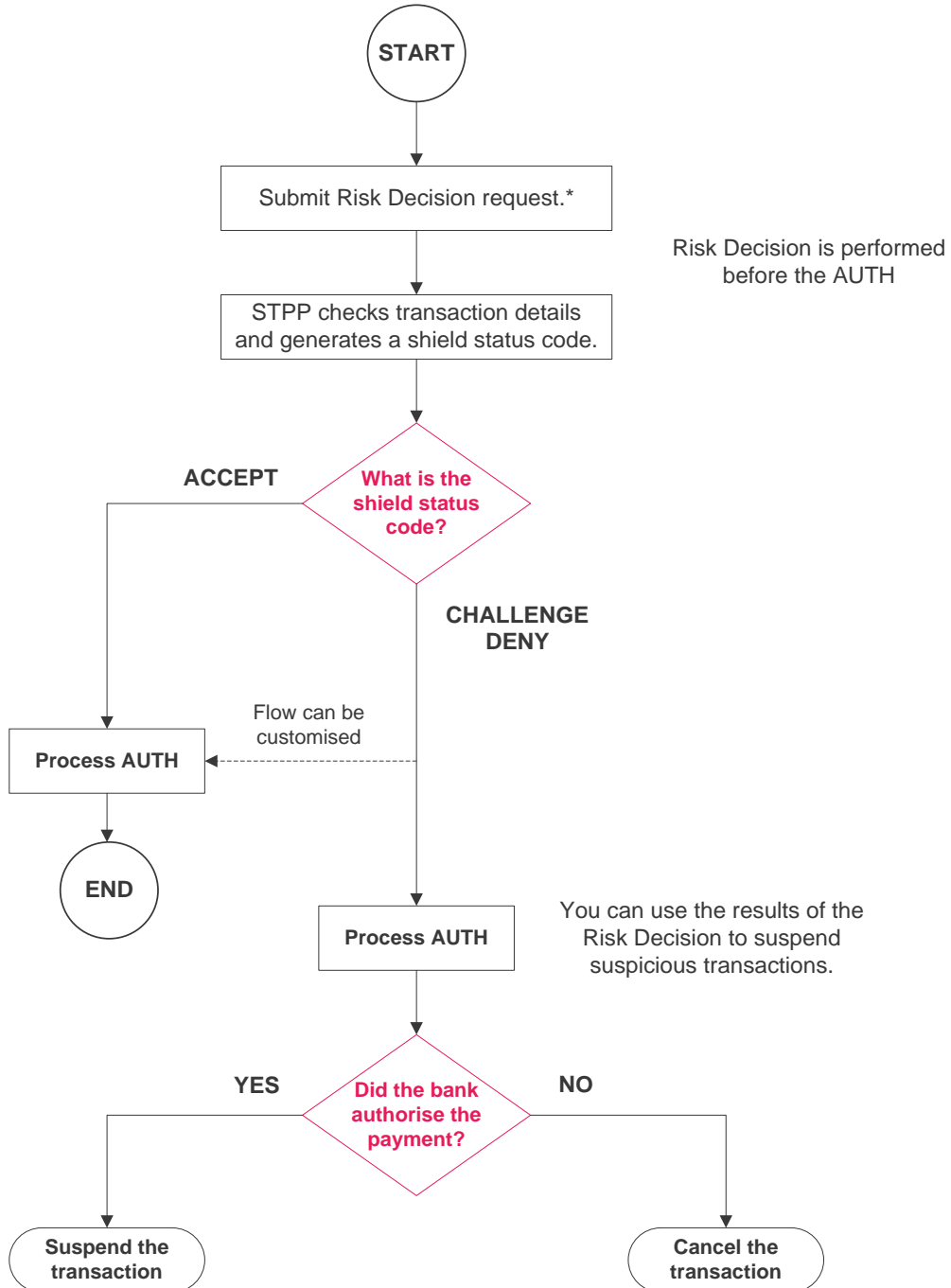
- // **ACCEPT** - The details are not deemed suspicious.
- // **DENY** - The details are suspicious and a transaction should not be performed.
- // **CHALLENGE** - Further investigation is recommended.
- // **NOSCORE** – Transaction was declined by the acquirer before checks were performed.

## 2 Process Overview

The two methods of performing Risk Decision requests are as follows:

### 2.1 Perform Risk Decision check first - Then seek authorisation

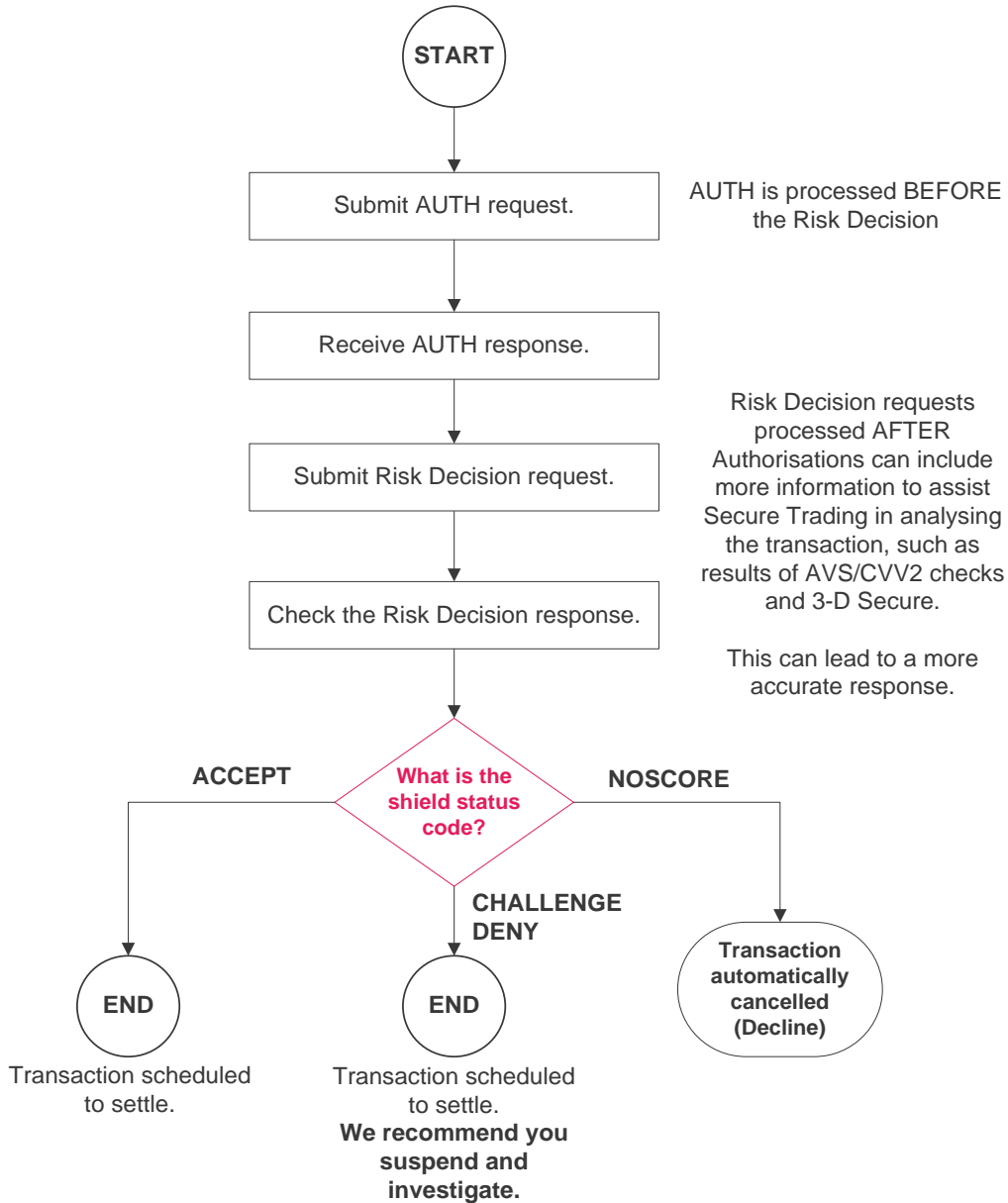
Supported interfaces: API & Payment Pages\*



\*Payment Pages interface: When enabled on your account, Risk Decision Requests are processed automatically without needing to change the POST to Secure Trading.

**2.2 Seek authorisation first - then perform a Risk Decision check**

Supported interfaces: API



**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 2.1.

### 3 Configuration



**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 more information, please contact the Secure Trading Sales team (see section 6.2).

#### 3.1 Payment Pages

To enable Protect Plus on your Secure Trading account, please contact the Secure Trading Sales team (see section 6.2). Once Protect Plus has been enabled, it will automatically be processed with every payment made through your payment page, without any additional configuration on your system.



For advanced functionality, Secure Trading offers an **Enhanced Post** feature, which allows you to choose which transactions are processed with Protect Plus. For more information, see the [Payment Pages Setup Guide](#).

#### 3.2 API

To enable Protect Plus on your Secure Trading account, please contact the Secure Trading Sales team (see section 6.2). Once Protect Plus has been enabled, you will need to configure your system to send Risk Decision requests to Secure Trading and interpret the responses returned.

For merchants using our XML interface, this is explained in depth in the [Protect Plus XML Specification](#).

## 4 Viewing the Results in MyST

Requests

- ALL
- ACCOUNTCHECK
- AUTH
- FRAUDSCORE
- REFUND
- RISKDEC
- THREEDQUERY

The results of Risk Decisions can be viewed in MyST. On the “**Transaction search**” page, select the “**RISKDEC**” filter (in the “Requests” pane) and click “**Search**” to search your site reference(s) for Risk Decision requests.

Security details

- Security response
- Shield status code
- Fraud rating
- Fraud reason

You can select the “**Shield status code**” field from the “Security details” pane to display this information in the search results.



**Please note** within MyST, the account type used for Protect Plus is referred to as “FRAUDCONTROL”.

The search results will look like this:

Display 10 transactions		Search: 2000-01-01 00:00 to 2014-12-16 23:59						
	Transaction ref	Account	Request	Timestamp	Amount	Site	Shield code	
<input type="checkbox"/>	7-65-254952	FRAUDCONTROL	RISKDEC	2014-12-12 11:16:00	£11.11	test_site12345	ACCEPT	
<input type="checkbox"/>	2-65-200855	FRAUDCONTROL	RISKDEC	2014-12-11 10:00:40	£11.11	test_site12345	ACCEPT	
<input type="checkbox"/>	3-65-252314	FRAUDCONTROL	RISKDEC	2014-12-10 15:33:00	£11.11	test_site12345	ACCEPT	
<input type="checkbox"/>	4-65-324042	FRAUDCONTROL	RISKDEC	2014-12-01 09:27:50	£11.33	test_site12345	CHALLENGE	
<input type="checkbox"/>	4-65-324039	FRAUDCONTROL	RISKDEC	2014-12-01 09:25:25	£11.22	test_site12345	DENY	
<input type="checkbox"/>	4-65-324032	FRAUDCONTROL	RISKDEC	2014-12-01 09:21:02	£11.11	test_site12345	ACCEPT	
<input type="checkbox"/>	2-65-194054	FRAUDCONTROL	RISKDEC	2014-12-01 09:05:48	£11.22	test_site12345	DENY	
<input type="checkbox"/>	6-65-325324	FRAUDCONTROL	RISKDEC	2014-12-01 09:01:43	£11.11	test_site12345	ACCEPT	
<input type="checkbox"/>	6-65-325322	FRAUDCONTROL	RISKDEC	2014-12-01 08:56:48	£11.33	test_site12345	CHALLENGE	
<input type="checkbox"/>	3-65-222767	FRAUDCONTROL	RISKDEC	2014-11-07 12:12:01	£11.11	test_site12345	ACCEPT	

Clicking on the transaction reference of one of the RISKDEC entries will take you to the single transaction view, which will contain more information. An example screenshot of this page can be found overleaf:

Protect Plus Guide

Transaction details		Related transactions	
<b>Transaction Details</b>			
Transaction reference	1-65-117	Parent	6-9-508353
Account	FRAUDCONTROL	Authorised amount	£11.33
Currency	GBP	Customer IP	1.2.3.4
Order reference			
<b>Payment Details</b>			
Payment type	VISA	Expiry date	10/2031
Card number	411111#####1111	Issuer	
Issuer country	ZZ		
<b>Risk Decision Details</b>			
Shield status code	CHALLENGE	Recommended action	C
ReD request ID	TEST	ReD order ID	000100000117
Response code	0330: A customized rule in the ReDShield Velocity Rules Engine returned a CHALLENGE response.		
Fraud category details			

When viewing details of a Risk Decision, the fields of specific interest can be found under the “Risk Decision Details” header (as shown in the screenshot, above).

These fields can be described as follows:

Field name	Details
Shield status code	One of the following: <b>ACCEPT</b> = The details are not deemed suspicious. <b>CHALLENGE</b> = Further investigation is recommended. <b>DENY</b> = The details are suspicious and a transaction should not be performed. <b>NOSCORE</b> = Returned when a parent Authorisation request has been declined.
ReD request ID	Unique Risk Decision request ID.
Response code	Response code relating to the Risk Decision check. See section 7.1.
Fraud category details	Reference used to identify a condition that was met in order to return the <b>DENY</b> or <b>CHALLENGE</b> shield status code.
Recommended action	One of the following: <b>C</b> = Continue with the transaction. <b>S</b> = Stop transaction.
ReD order ID	Unique Risk Decision order ID.



More details on viewing request details using MyST can be found in the [MyST User Guide](#).  
All Secure Trading documents can be found on [our website](#).



## 5 Additional Notes

### 5.1 Supported Payment Types

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

### 5.2 3-D Secure Support

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

#### 5.2.1 Merchants using our API

Information on whether or not the customer is enrolled in 3-D Secure can be used by the Protect Plus system (when a Risk Decision request is performed after an Authorisation request, section 2.2) to assist you in deciding whether or not to proceed with the transaction.

For instructions on integrating Risk Decision into your 3-D Secure XML solution, please consult the [3-D Secure](#) and [Protect Plus](#) XML reference documents.

### 5.3 Testing

The following main amounts can be submitted to test the different Protect Plus Risk Decision responses:

Risk Decision Response	Main Amount
<b>ACCEPT</b>	11.11
<b>CHALLENGE</b>	11.33
<b>DENY</b>	11.22

For greater detail on how to test your implementation, please refer to the [Testing document](#).

## 6 Further Information and Support

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

### 6.1 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	<a href="mailto:support@securetrading.com">support@securetrading.com</a>
Website	<a href="http://www.securetrading.com/support/support.html">http://www.securetrading.com/support/support.html</a>

### 6.2 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	<a href="mailto:sales@securetrading.com">sales@securetrading.com</a>
Website	<a href="http://www.securetrading.com">http://www.securetrading.com</a>

### 6.3 Useful Documents

The following documents should be read in conjunction with this document:

- # [STPP Payment Pages Guide](#) – This document outlines how to use Payment Pages to process payments on your website.
- # [STPP MyST User Guide](#) – This document outlines how to use MyST to monitor your transactions and manage your account.
- # [STPP XML Specification](#) – This document details the structure of AUTH, REFUND and ACCOUNTCHECK XML Requests and Responses processed through Secure Trading.
- # [STPP Protect Plus XML Reference](#) - This document explains RISKDEC XML Requests and Responses processed through Secure Trading.
- # [STPP 3-D Secure XML Reference](#) - This document explains THREEDQUERY XML Requests and Responses processed through Secure Trading.
- # [STPP Testing Document](#) - This document provides an overview on testing your Secure Trading solution.

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

### 6.4 Frequently Asked Questions

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

## 7 Appendix

### 7.1 Response Codes

The value returned in the “Response code” field in MyST, 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.