



## **VSP Direct Protocol and Integration Guidelines**



## Document Index

Welcome to VSP Direct.....	3
Overview of how VSP Direct Payments work.....	4
VSP Direct and 3D-Secure .....	5
The VSP Direct Payment Process in Detail .....	7
Step 1: The customer orders from your site. ....	7
Step 2: Your server registers the payment with Protx. ....	8
Step 3: VSP Direct and Protx MPI check 3D-Secure status. ....	10
Step 4: VSP Direct replies to your registration POST. ....	11
Step 5: You redirect your customer to their Issuing Bank. ....	12
Step 6: 3D-Authentication is carried out and your site called back. ....	13
Step 7: Your site POSTs the 3D-Secure results to Protx.....	14
Step 8: VSP Direct requests card authorisation. ....	15
Step 9: Protx reply to your server's POST. ....	16
Step 10: VSP sends daily Batch File to confirm payments. ....	17
Integrating with VSP Direct.....	18
Stage 1: Integrating with the VSP Simulator .....	20
1: VSP Simulator Account Set up .....	21
2: VSP Direct Set up .....	22
3: Registering a Payment.....	23
4: 3D-Authenticated Transactions .....	25
5: Examining your transactions .....	26
6: Additional Transaction Types .....	27
Stage 2: Testing on the Test Server .....	31
The Test Server VSP Admin.....	33
Appendix A – The VSP Direct Protocol v2.22.....	38
A1: Transaction registration .....	38
A2: Protx Response to the Transaction Registration or Callback POSTs .....	42
A3: 3D-Authentication Results POST from your Terminal URL to Protx.....	45
A4: Response to 3D Callback POSTs .....	45
A5: VSP Direct Full URL Summary.....	45



## Welcome to VSP Direct

The Protx Veri-Secure Payment system (VSP) provides a secure, simple means of authorising credit and debit card transactions from your web site.

VSP Direct is designed to enable you to take card details on your own secure servers and pass them across to us for authorisation and secure storage in a server-to-server session that does not involve redirecting the customer to the Protx pages. This enables you to white-label the payment process. Your customer never leaves your site (unless you are using the 3D-Secure authentication processes) and they do not necessarily know that that Protx is authorising the transaction on your behalf (although in practice many merchants chose to tell their customers in case they have concerns about card number security).

To use VSP Direct you will need a 128-bit SSL certificate to secure your payment pages. These can be obtained from a number of sources including VeriSign and Thawte. You will also need to be able to make HTTPS POSTs from scripts on your server (using something like OpenSSL on Linux platforms, or the WinHTTP object in Win32). If you are hosting with a third party company we recommend you talk to them about these requirements before committing to use VSP Direct. If you cannot install a certificate for your payment pages, we would recommend using VSP Server instead. If you cannot perform HTTPS POSTs from your scripts, we would recommend VSP Form.

If you wish to support Verified by Visa and MasterCard SecureCode (the cardholder authentication systems collectively known as 3D-Secure), VSP Direct provides a wrapper for these systems, removing the need for you to purchase and support your own Merchant Plug-In. All the messages will be created for you, and you'll simply need to redirect your customer to their issuing bank, then send on the results of their 3D-Authentication back to VSP Direct to complete the payment process. Just like non 3D-Secure VSP Direct transactions, the customer is never directed to Protx. They leave your site to authenticate with their bank, then return to your site when they have finished.

This document explains how your Web servers communicate with VSP Direct, goes on to explain how to integrate with our testing and live environments, and contains the complete Payment Protocol in the Appendix.

PLEASE NOTE: Originally the Protx VSP product was called the "Verified Payment System" and was referred to by the acronym VPS. When the product expanded to support a variety of interfaces, the name was changed to reflect the type of interface used. When reference is made to VPSTxId or VSPProtocol, these are not transposition errors. These field names date back to the original system.



## Overview of how VSP Direct Payments work

VSP Direct payment requests are very simple. The interaction with your customer is entirely yours. The customer will select items or services to purchase and fill up a shopping basket. When they are ready to pay, you will first collect their name, delivery address, contact details (telephone number, e-mail address and so forth) and perhaps allow them to sign up for quicker purchases in future. You will total the contents of the basket and summarise its contents for them before asking them to continue.

Your scripts should then store everything about the transaction and customer in your database for future reference. You will not need to store any card details because Protix will hold those securely for you.

You will then present your customers with a payment page, secured with your 128-bit SSL certificate. This page will ask the customer for:

- The Cardholder Name as it appears on the card
- The Card Type (Visa, Mastercard, American Express etc.)
- The full Card Number without spaces or other separators
- The Start Date (if printed on the card)
- The Expiry Date
- The Issue Number (for some Maestro and Solo cards only)
- The Card Verification Value (called CVV or CV2 value. The extra three digits on the signature strip or most cards, or the 4 numbers printed on the front of an American Express card).
- The Card Holder's Billing Address, including the Post Code (if you have not already asked for it and stored it in your database).

This page is submitted to a script on your server that retrieves and pre-validates those values (checking all fields are present, expiry dates are not in the past, the card number field only contains numbers etc.) before constructing a HTTPS POST containing your own unique reference to the transaction, the VendorTxCode (which should be stored alongside the order details in your database) and the correctly formatted data from your form. This HTTPS POST is sent to the Protix VSP Direct gateway.

Protix validate the data sent to us, checking that it has come from a valid source and that all required information is present, before creating a transaction in our database to securely hold all the data passed to us, contacting the bank for authorisation and replying to you, in real-time, in the response part of the same HTTPS POST. In practise this takes about 2-3 seconds to complete.

The same script on your server that initiated the POST simply reads the Response from that POST to determine whether the transaction was authorised or not. It then updates your database with transaction references value and the authorisation code (where appropriate) before displaying either a completion page to your customer, or an error page explaining why the payment was not accepted.



Your own database will contain all the necessary information about the transaction, the basket contents and the customer, but you will NOT need to store the card details because the transaction ids passed to you by the VSP Direct system will enable you to perform all other actions against that card (refunds, additional payments, cancellations and so on). This allows you to be certain that even if your server is compromised, no card details can be gleaned from your database.

The following sections explain the integration process in more detail. The VSP Direct Payment protocol is attached in the appendix, providing a detailed breakdown of the contents of the HTTPS message sent between your servers and ours during a payment.

A companion document, "VSP Server and Direct Shared Protocols", gives details of how to perform other transaction related POSTs, such as Refunds, Repeat payments and the Release/Abort mechanisms for Deferred transactions.

## VSP Direct and 3D-Secure

VSP Direct payments with 3D-Authentication are a little more complicated because your customer has to be forwarded to their card issuer to authenticate themselves BEFORE a card authorisation can occur. You must have 3D-Secure active on your account before you can process this type of transaction. Contact [info@protx.com](mailto:info@protx.com) for more information about setting this up.

The process of obtaining a 3D-Secured authorisation begins in the same manner as non-authenticated transactions. Your customer fills up a shopping basket on your site, you collect their details, then present them with a payment page secured with your 128-bit SSL certificate. This page POSTs to a script on your site which pre-validates the data and formats a normal server-side VPS Direct transaction registration POST (see Appendix A) which is sent to Protx.

As in a non-authenticated VSP Direct transaction, the information you POST to us is validated against your valid IP addresses and the data checked for range errors, but if everything appears in order, rather than immediately sending the card details to your acquiring bank for authorisation, the details are instead used to send a query to the 3D-Secure directory servers. These check to see if the card and the card-issuer are enrolled in the 3D-Secure scheme.

If the card or the issuer is NOT part of the scheme, VSP Direct checks your 3D-Secure rule base (which you can modify in our VSP Admin screens) to determine if you wish to proceed with the authorisation in such circumstances. If authorisation can proceed, the card details are sent to the acquiring bank and the results of that process returned to your site in the Response object of your POST (just like a non-3D-authenticated VSP Direct transaction, but with an additional 3DSecureStatus field informing you about the results of the card lookup).

If authorisation cannot proceed because your rules do not allow it, a **REJECTED** message is sent back in the Response object of your POST, outlining the reason for the transaction rejection.



If, however, the card AND issuer are part of the 3D-Secure scheme, VSP Direct does not attempt to obtain an authorisation from your acquiring bank. Instead it formats and encrypts a 3D-Secure request message called a **PAReq** and replies to your VSP Direct POST in the Response object with this message, a unique transaction code called the **MD**, and the URL of the 3D-Secure authentication pages at the cardholder's Issuing Bank (in a field called **ACSURL**). You do not need to store any of these details in your database.

Your server creates a simple, automatically-submitted HTML form that POSTs the user, the MD and the PAReq fields across to the ACSURL. From the user's perspective, they will have entered their card details on your payment page, clicked submit, and will find themselves transferred to their card issuer to validate their 3D-Secure credentials.

Once the user has completed their 3D-authentication, their Issuing Bank will redirect the customer back to a script on your site called your Terminal URL (or **TermURL**). You supply this URL in the redirection form above. The user returns to your site along with the **MD** of the transaction and the results of their authentication in an encrypted field called the **PARes**. Like before, VSP Direct takes care of decrypting and decoding this information for you, so your Terminal URL page simply formats a server side HTTPS POST containing the MD and the PARes fields and sends it to the VSP Direct Callback URL. You do not need to store the MD or PARes fields in your database

VSP Direct examines the PARes to determine if authentication was successful. If it was, it retrieves all the details of your original VSP Direct POST and goes on to obtain an authorisation from your Issuing Bank. It then replies with the results in the Response object of your Terminal URL POST in the same format as non-3D secured transaction, but with two additional fields for you to store (the **3DSecureStatus** and the **CAVV** value; a unique value which indicates that the Authentication was successful).

If VSP Direct examines your PARes and finds that authentication was NOT successful, it again checks your 3D-Secure rule base to determine if you wish to proceed. Like the original transaction registration POST, if you do wish to obtain authorisations for non-3D-authenticated transactions, VSP Direct requests an authorisation from your acquiring bank and replies as normal; if not, VSP Direct returns a **REJECTED** message and does not obtain an authorisation.

Your Terminal URL should update your database with the results of the authorisation (or lack thereof) and display a completion page to your customer.

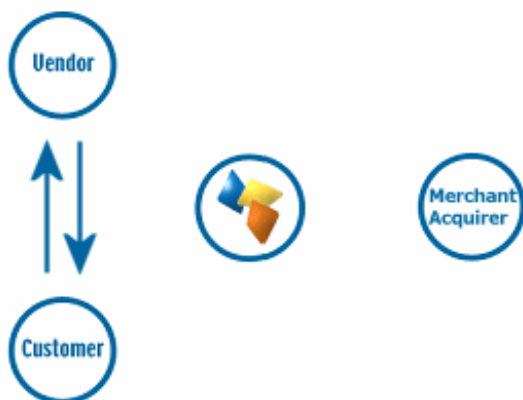
Although more complex than a non-3D-authenticated VSP Direct transaction, this process does remove a huge amount of the complexity involved in using your own Merchant Plug-In. Moreover, transactions which fully authenticate offer you the protection of a liability shift for card related misuse, which is extremely useful if you sell products or services that attract fraudsters.



## The VSP Direct Payment Process in Detail

This section defines the messages exchanged between your Web servers and the VSP Direct system.

### Step 1: The customer orders from your site.



A payment begins with the customer ordering goods or services from your site. This process can be as simple as selecting an item from a drop down list, or can involve a large shopping basket containing multiple items with discounts and delivery charges. Your interaction with your customer is entirely up to you and the VSP Direct system puts no requirement on you to collect any specific set of information at this stage.

It is generally a good idea to identify the customer by name, e-mail address, delivery and billing address and telephone number. It is also helpful to have your server record the IP Address from which the customer is accessing your system. You should store these details in your database alongside details of the customer's basket contents or other ordered goods.

You then present a 128-bit SSL secured payment page into which the customer can enter their card and billing address details. This page should contain the following fields.

- The Cardholder Name as it appears on the card
- The Card Type (Visa, MasterCard, Delta, Maestro, Solo, Electron, American Express, Diners Club or JCB)
- The full Card Number without spaces or other separators
- The Start Date (if printed on the card)
- The Expiry Date
- The Issue Number (for some Switch and Solo cards only)
- The Card Verification Value (called CVV or CV2 value. The extra three digits on the signature strip or most cards, or the 4 numbers printed on the front of an American Express card).
- The Card Holder's Billing Address, including the Post Code (if you have not already asked for it and stored it in your database).

If you wish to provide list boxes for Start and Expiry Dates, please be aware that Visa now issue cards valid for up to 20 years.





## Step 2: Your server registers the payment with ProtX.



Once the user has clicked Continue, a script on your web server will construct a payment registration message (see Appendix A1) and POST it via HTTPS to the VSP Direct payment URL.

This POST contains your **VSP Vendor Name** (chosen by you on the ProtX online application form, or assigned to you by ProtX when your account is created) and your own unique reference to this payment (in a field called **VendorTxCode**, which you must ensure is a completely

unique value for each transaction)

The message also contains the total value and currency of the payment, and billing address details for the customer. You can specify a brief description of the goods bought to appear in our reports, plus the entire basket contents if you so wish. The card details themselves are passed in dedicated fields whose format can be found in appendix A1.

In the VSP 2.22 protocol you can also pass delivery address details, contact numbers and e-mail addresses, flags to bypass or force fraud checking for this transaction and 3D-Secure reference numbers and ids where such checks have been carried out.

Because this message is POSTed directly from your servers to ours across a 128-bit encrypted session, no sensitive information is passed via the customer's browser, and anyone who attempted to intercept the message would not be able to read it. Using VSP Direct you can be assured that the information you send us cannot be tampered with or understood by anyone other than us. Your script sends the payment registration message in the Request object of the HTTPS POST and the response from our server (see steps 4 and 9 below) in the Response object of the same POST is in real time.

On receipt of the POST, VSP Direct begins by validating its contents.

It first checks to ensure all the required fields are present, and that their format is correct. If any are not present or contain the wrong type of data, a reply with a **Status** of **MALFORMED** is generated, with the **StatusDetail** field containing a human readable error message. This normally only happens in the development stage.

If all fields are present and correct, the information in those fields is then validated. The Vendor name is checked against a pre-registered set of IP addresses, so VSP Direct can ensure the POST came from a recognised source. The currency of the transaction is validated against those accepted by your merchant accounts. The VendorTxCode is checked to ensure it has not been used before. The card number is checked against the card type to ensure that it is of the type selected and all associated fields are checked to ensure the card is still active. The amount field is



# VSP Direct Protocol and Integration Guidelines



validated. Flag fields are checked... every field, in fact, is checked to ensure you have passed the correct values. If any of the information does not check out, a reply with a **Status** of **INVALID** is returned, again with a human readable error message in **StatusDetail**.

If you receive either a MALFORMED or INVALID message you should use the detailed response in the StatusDetail error message to help debug your scripts. If you receive these messages on your live environment, you should inform your customer that there has been a problem registering their transaction, then flag an error in your back-office systems to help you debug. You can e-mail the Protix Support team ([support@protix.com](mailto:support@protix.com)) for help with your debugging issues.

In practise you only normally receive MALFORMED and INVALID messages during development, whilst you are ironing out bugs in your scripts, but your site should be able to handle such errors in case they occur once your site is live.

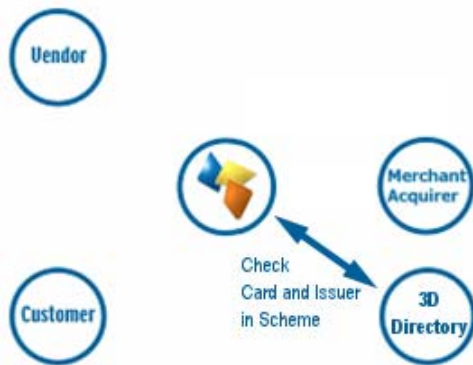
The integration kits we provide contain scripts in a variety of languages that illustrate how you compose and send this message from your server to ours. . These can be downloaded as part of the application process or obtained from the <http://techsupport.protix.com> downloads area.

When your transaction is registered with the VSP Direct system, a new transaction code is generated that is unique across ALL vendors using the VSP systems, not just unique to you. This code, the **VPSTxid**, is our unique reference to the transaction and is returned to you in the response part of the POST after we've requested authorisation for you. This reference, whilst not the most easily remembered number, will allow us to immediately find your transaction if you have a query about it.

If your Protix account is not set up with 3D-Secure or 3D-Authentication is not active for this VSP Direct transaction, the next step is for the system to obtain an authorisation, so skip ahead to step 8. If, however, 3D-Secure is active on your account, continue at step 3.



## Step 3: VSP Direct and Protix MPI check 3D-Secure status.



VSP Direct sends the card details provided in your post to the Protix 3D-Secure Merchant Plug-In (MPI). This formats a request called a VEReq, which is sent to the 3D-Secure directory servers to query whether the card and card issuer are part of the 3D-Secure scheme.

The servers send a VERes response back to the MPI where it is decoded and VSP Direct informed of the inclusion or exclusion of the card.

If the card or the issuer is not part of the scheme, or if an MPI error occurs, VSP Direct will check your 3D-Secure rule base to determine if authentication should occur. By default you will not have a rule base established and transactions that are not, or cannot, be 3D-authenticated will still be forwarded to your acquiring bank for authorisation.

If you do have a rule base, the value of the transaction and the AllowCardNotInScheme, AllowIssuerNotInScheme and AllowMPIErrors flags will determine if authorisation should be attempted.

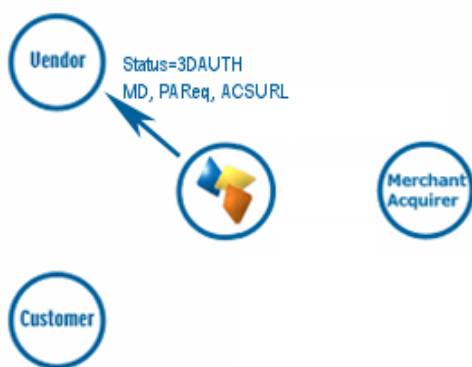
If your rulebase rejects the transaction due to your criteria not being reached, VSP Direct replies with **Status** of **REJECTED** and **StatusDetail** indicating why. The **3DSecureStatus** field will contain the results of the 3D-Secure lookup. REJECTED transactions will never be authorised and the customer's card never charged, so your code should redirect your customer to an order failure page, explaining why the transaction was aborted.

If your rule base DOES allow authorisation to occur for non-3D-authenticated transactions, VSP Direct continues as though 3D-Secure is not active on your account. Jump ahead to step 9 in these circumstances for the authorisation stage.

If the card and the card issuer are both part of the scheme, VSP Direct continue with 3D-Authentication by replying to your post with a **Status** of **3DAUTH** (see the next step)



## Step 4: VSP Direct replies to your registration POST.



VSP Direct stores all the information from your transaction registration POST in the Protx secure database before replying to that POST with 6 fields (see Appendix A2). The **Status** field will be set to **3DAUTH** with a **StatusDetail** informing you to redirect your customer to their Issuing Bank to complete 3D-Authentication.

A unique identifier to your transaction called the **MD** is passed along with a preformatted, encrypted field called **PAREq**. This is the 3D-Secure message that the customer's card

Issuing Bank decodes to begin the 3D-authentication process. This is created and encrypted by the Protx MPI and you should not attempt to modify it. If you do, the 3D-Secure authentication step will fail and this, in turn, will fail your transaction.

A field called **ACSURL** contains the fully qualified address of the Issuing Bank's 3D-Secure module, as provided by the directory service in the VERes (see step 4 above). The last field is the **3DSecureStatus** field, which will always contain **OK** for transactions ready for authentication.

You do not need to store any of these values in your database. You can store the MD value if you wish, but the ACSURL and PAREq values should NEVER be stored. Doing so would require you to undergo auditing by the card scheme, so unless you are already PCI-DSS compliant, you should avoid doing this. These values only need to be used in the next step to redirect your customer to their Issuing Bank and should then be discarded.

The first step of the VSP Direct transaction is now complete. You have registered a 3D-Secure transaction with Protx, we have stored your payment details and replied with everything you need to send your customer for 3D-Authentication. The next parts of the process, steps 5 to 7, are out of our control and rely on a communication between you, your customer and your customer's card Issuing Bank.



## Step 5: You redirect your customer to their Issuing Bank.



The registration page code on your server should check the **Status** field, and when a **3DAUTH** status is found, build a simple, auto-submitting form (see the example below) which sends the **MD**, **PaReq** and an additional field, the **TermUrl**, to the address specified in the **ACSURL**, and send this form to your customer's browser.

This has the effect of redirecting your customer to their card Issuer's 3D-Authentication site whilst sending to that site all the information required to perform the authentication.

The **TermURL** field is a fully qualified URL which points to the page on your servers to which the customer is sent once the 3D-authentication is completed (see step 6 below). Example code for this page is included in the integration kits provided by ProtX. It just needs to be an SSL-Secured script that can accept connections from the Internet.

As mentioned above, this redirection of your customer is achieved with a simple, automatically submitting form sent to their browser. Your script should clear the response object of any output, then send something like the following HTML code:

```

<SCRIPT LANGUAGE="Javascript">
function OnLoadEvent() { document.form.submit(); }
</SCRIPT>

<html><head><title>3D Secure Verification</title></head>
<body OnLoad="OnLoadEvent();">
<FORM name="form" action="{ACSURL}" method="POST"/>
<input type="hidden" name="PaReq" value="{PAREQ}"/>
<input type="hidden" name="TermUrl" value="{Your Terminal URL Page}"/>
<input type="hidden" name="MD" value="{MD}"/>
<NOSCRIPT>
<center><p>Please click button below to Authenticate your card</p><input type="submit"
value="Go"/></p></center>
</NOSCRIPT>
</form></body></html>
    
```

The values in Red are those extracted from the ProtX response and built by your script. If your user has Javascript enabled, they simply redirect to their Issuing Bank site. If not, they will be presented with the message in the NOSCRIPT section and need to click it to go to their Issuing Bank.

At this stage the customer has left your site, and you must wait for them to be sent back to you by the Issuing Bank.



NOTE: You can either redirect the customer's entire browser page to their issuing bank ACSURL, or more commonly, use an inline frame to redirect them. Visa recommend using inline frames for continuity of customer experience, but if you do so, remember to add code to support IFRAME incapable browsers.

ADDITIONAL IMPORTANT NOTE: When you forward the PAREq field to the ACSURL, please ensure you pass the PAREq value that we send you, in a field called **PaReq** (note the lower case "a"). Many ACSURL pages are case sensitive, and will not see the data if you pass an upper case A. See the example code above for how to submit the data.

## Step 6: 3D-Authentication is carried out and your site called back.



Your customer completes the 3D-authentication process at their Issuing Bank's web site.

Once complete (either successfully or not), the bank will redirect your customer back to the page supplied in the **TermURL** field you sent in step 5 above.

Along with this redirection, two fields are also sent. The **MD** value, to uniquely identify the transaction you are being called back about, and the **PAREs**, the encrypted

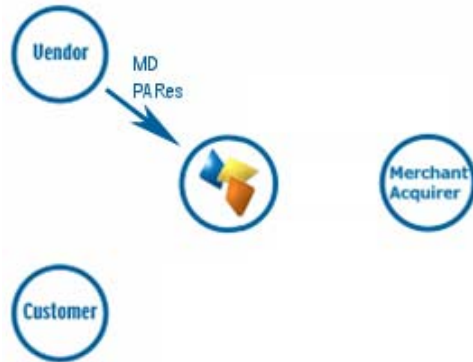
and encoded results of your customer's 3D-authentication.

Like the PAREq value sent to your site by ProtX in step 5, you should NOT store the PAREs file in your database. Also, because it is strongly encrypted, only the ProtX MPI can decode this for you, so you should not attempt to modify it or the authentication process will fail.

At this stage the customer is back on your site and you have completion information for the 3D-Authentication process. You now need to send those through to ProtX to decode the results and, where appropriate, obtain a card authorisation from your acquiring bank.



## Step 7: Your site POSTs the 3D-Secure results to Protx.



The code in your call back page should format a simple HTTPS, server-side POST, which it sends to the Protx VSP Direct 3D-Callback page.

This POST needs to contain the **MD** and **PAREs** fields sent back to your site by the cardholder's Issuing Bank.

No other information is necessary because the Protx system can use these values to retrieve all the transaction information you

originally supplied.

If the decoded PAREs indicates that the 3D-Authentication was successful, VSP Direct goes on to obtain an authorisation (see the next step). If not, the system examines your 3D-Secure rule base to see if authentication should be attempted. By default 3D-Authentication failures are NOT sent for authorisation, but all other message types are. Refer to the Protx Rulebase guide for more information about using 3D-Secure and AVS/CV2 rules.

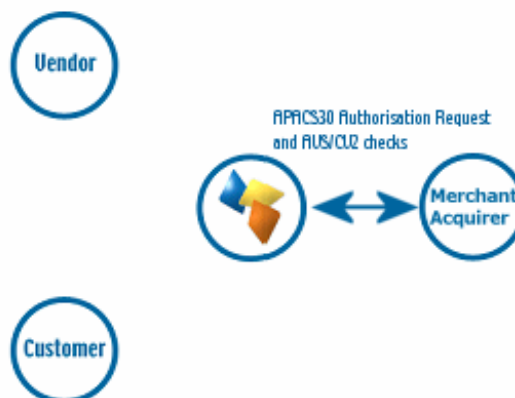
Transactions not sent for authorisation are returned with a **REJECTED** status.



## Step 8: VSP Direct requests card authorisation.

The VSP services format a bank specific authorisation message (including any 3D-Secure authentication values where appropriate) and pass it to your merchant acquirer over the private banking network.

The request is normally answered within two seconds with either an authorisation code, or a failure message (at busy times of year, this process can take up to 60 seconds, but that is increasingly rare).



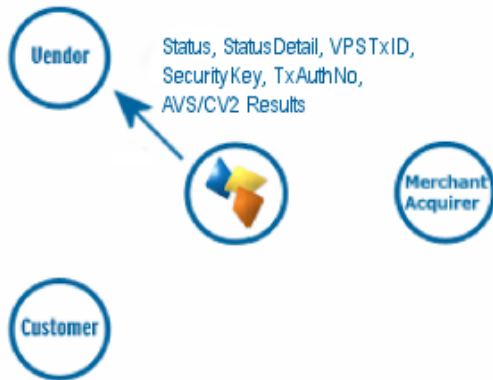
This process happens in real-time whilst the script on your server is waiting for a response from VSP Direct. Depending on the response from the acquirer, VSP Direct prepares either an **OK** response with an Authorisation Code, a **NOTAUTHED** response if the bank declined the transaction or an **ERROR** if something has gone wrong (you will very rarely receive these except during planned outages and upgrades).

If AVS and CV2 checks are being performed, the results are compared to any rule bases you have set up (see the ProtX Rulebase Guide for more information). If the bank has authorised the transaction but the card has failed the AVS and/or CV2 rules you have established, ProtX immediately reverse the authorisation on the card and prepare a **REJECTED** response, returning the reason for the failure in the AVSCV2 field.





## Step 9: Protx reply to your server's POST.



Irrespective of the Status being returned, VSP Direct always replies in the Response section of the POST that your server sent to us. This will either be in response to the transaction registration POST for non-3D-authenticated transactions, or in the response to the Terminal URL POST if 3D-Authentication was attempted.

If the transaction was registered successfully, you will always receive the **VPSTxId**, the unique transaction reference mentioned above.

You will also receive a **SecurityKey**, a 10-digit alphanumeric code that is used in digitally signing the transaction. Whilst not used in the VSP Direct messages, you do need to know this value if you wish to REFUND the transaction, or perform any other actions on it using the VSP Server interface. Therefore this value should be stored alongside the **VPSTxId**, the order details and the **VendorTxCode**, in your database.

If the transaction was authorised and the Status field contains **OK**, you will also receive a field called **TxAuthNo**. The TxAuthNo field DOES NOT contain the actual Authorisation Code sent by the bank, because it is not unique (although we do store this in our system for you), but contains instead a unique reference number to that authorisation that we call the **VPSEAuthCode**. This is the transaction ID sent to the bank during settlement (we cannot use your VendorTxCode because it is too long and might contain invalid characters) so the bank will use this value to refer to your transaction if they need to contact you about it. You should store this value in your database along with all the other values returned to you.

The TxAuthNo field is ONLY present if the transaction was authorised by the bank. All other messages are authorisation failures of one type or another (see Appendix A2 for full details of the fields and errors returned by VSP Direct) and you should inform your customer that their payment was not accepted.

If you do receive an **OK** status and a **TxAuthNo**, you should display a completion page for your customer thanking them for their order.

Having stored the relevant transaction ids in your database, your payment processing is now complete.



## Step 10: VSP sends daily Batch File to confirm payments.



Once per day, at 2:00am, the VSP Server system batches all authorised transactions for each acquirer and creates a bank specific settlement file.

Transactions for ALL merchants who use the same merchant acquirer are included in this file. Every transaction from 00:00:00am until 11:59:59pm on the previous day is included in the files.

They are uploaded directly to the acquiring banks on a private secure connection. This process requires no feedback or input from you or your site.

If the file does not transmit correctly, the system tries a further nine times at 10-minute intervals. If all 10 attempts fail the transactions for that bank are rescheduled for inclusion in the following day's batch instead. Protx monitor this process each day to ensure the files have been sent, and if not, the support department correct the problem during the day to ensure the file is sent correctly that evening (or normally resubmit the file manually the same day to ensure funds are available to all vendors more expediently).

The acquirers send summary information back to ProtX to confirm receipt of the file, then later more detailed information about rejections or errors. If transactions are rejected, we correct any errors and resubmit them for you. Your bank will contact you directly if there are any non-formatting related problems with the transactions.



## Integrating with VSP Direct

Linking your Web site to VSP Direct involves creating one script (or modifying the example provided in the integration kits), which both registers the transaction with our servers and processes the response we send back. If you wish to support 3D-Secure Authentication, you will also need to create or modify a second script to handle the call back from the Issuing Bank.

### Stage 1

The VSP Simulator system is the starting point for your integration. This user-friendly expert-system on our test environment analyses the messages your site sends to us, reports any errors therein, and simulates all possible responses from the real VSP Direct and 3D-authentication systems.

The VSP Simulator can be configured on the following URL:

<https://ukvpstest.protx.com/VSPSimulator>

Payment transactions should be sent from your scripts to the following URL:

<https://ukvpstest.protx.com/VSPSimulator/VSPDirectGateway.asp>

3D-secure callback POSTS should be sent to the following URL:

<https://ukvpstest.protx.com/VSPSimulator/VSPDirectCallback.asp>

### Stage 2

Once your site is able to talk to VSP Simulator and process all possible outcomes, an account will be created for you on the VSP Test Server. This is an exact copy of the live site but without the banks attached and with a simulated 3D-Secure environment. Authorisations on the test server are only simulated, but the user experience is identical to Live, and a version of the VSP Administration pages also run here so you can familiarise yourself with the features available to you.

The VSP Admin system for viewing your Test transactions is at:

<https://ukvpstest.protx.com/VSPAdmin>

Transactions from your scripts should be sent to the Test Site VSP Direct at:

<https://ukvpstest.protx.com/vspgateway/service/vspdirect-register.vsp>

3D-secure callback POSTS should be sent to the following URL:

<https://ukvpstest.protx.com/vspgateway/service/direct3dcallback.vsp>

# VSP Direct Protocol and Integration Guidelines



## Stage3

Once you are happily processing end-to-end transactions on the test server and we can see test payments and refunds going through your account, AND you've completed the online Direct Debit signup, you send a Go Live request to [golive@protx.com](mailto:golive@protx.com) and we set up your account on our live servers. You then need to redirect your scripts to send transactions to the live service, send through a Payment using your own credit card, then VOID it through the VSP Admin service so you don't charge yourself. If this works successfully, then you are ready to trade online.

The Live VSP Admin screens are at:

<https://ukvps.protx.com/VSPAdmin>

Transactions from your scripts should be sent to the Live Site VSP Server at:

<https://ukvps.protx.com/vspgateway/service/vspdirect-register.vsp>

3D-secure callback POSTS should be sent to the following URL:

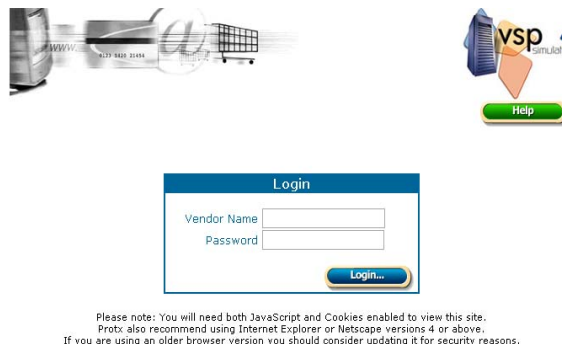
<https://ukvps.protx.com/vspgateway/service/direct3dcallback.vsp>



## Stage 1: Integrating with the VSP Simulator

The VSP Simulator is an expert system that emulates the VSP Direct system and allows you to develop your site to correctly send and process the messages exchanged between your site and ours. VSP Simulator will provide more detailed feedback of any errors or issues than the real VSP Direct, allowing you to debug and enhance your code at an earlier stage.

Log into VSP Simulator at <https://ukvpstest.protx.com/VSPSimulator> and enter your VSP Vendor Name (as you selected on the Online Registration forms) and the password (also the same as that used on those forms. You can change it in the Simulator if you wish).



If you have not yet completed the online registration forms, you need to progress at least as far as the Merchant Account section (i.e. complete all sections up to and including the Technical section) before a VSP Simulator account is automatically created for you. The Online Registration Forms are at <https://support.protx.com/apply>

When you log in to VSP Simulator you will be presented with the main menu screen. Extensive help is provided in the Simulator (click the context sensitive Help button on each screen for more details). This document will not cover everything in too much detail, but outlined in subsequent sections are the important steps you should take to get your site talking to the Simulator.





## 1: VSP Simulator Account Set up

Click the Account button in the main menu to open the following screen:

The screenshot shows the 'VSP Simulator account for Tony's Toupees' interface. It includes a 'Logout' button and a 'Help' button. The main section is titled 'Administrative Functions - Account Administration' and contains several sub-sections:

- Account Settings:** A form with fields for 'Company Display Name' (Tony's Toupees), 'Full Home Page URL' (http://www.protx.com), and 'Your contact e-mail address' (Tony.Welch@protx.com). It also has checkboxes for 'Simulate VSP Form', 'Simulate VSP Server' (checked), 'Simulate VSP Direct', and 'Enable PREAUTH & REPEAT transactions'. There are dropdown menus for 'Operating System' (none selected), 'Scripting Language' (ASP), and 'Shopping Cart Used' (none selected). An 'Update' button is at the bottom right.
- Valid IP Addresses for this Account:** A section explaining that these IP addresses list ONLY those servers at your site which DIRECTLY connect to either VSP Server or VSP Direct. It shows a 'PROTX Internal IP Address for VSP Admin' (213.052.206.220) and a 'Delete' button. Below is a form to 'Add New IP' and 'Subnet Mask' with an 'Add' button.
- Valid Currencies for this Account:** A section explaining that only transaction registrations for amount in the following Currencies will be accepted by the VSP Simulator. It shows a 'Delete' button and a form to 'Add New Currency' (AUD - Australian Dollar) with an 'Add' button.
- Change Password:** A form with fields for 'Current Password', 'New Password', and 'Confirm New Password', with a 'Set Password' button.

At the bottom, there is a 'Back' button and a note: 'Click the Back button to go back to the main menu.'

You should ensure that:

- all company details are correct.
- all technical details about web server and platform are correct.
- the VSP Direct box is checked.
- all relevant payment types have been set up.
- you have at least one payment currency set up (usually GBP unless your site take multi-currency transactions).
- the IP addresses of your servers are listed.

Add and/or correct any entries and click the Update button to save any changes. Back takes you back to the main menu.



## 2: VSP Direct Set up

Click the VSP Direct button in the main menu to open the VSP Server options page.

**VSP Simulator account for Matty's Marvellous Medicine Ltd**

[Logout](#) [Help](#)

**VSP Direct - Options and Parameters Page**

This page allows you to configure the VSP Simulator to respond in the manner you wish when VSP Direct messages are sent to the system. The Simulator will validate the data you send in the POST and always return **MALFORMED** or **INVALID** if the data is incorrect. You can force those responses if you wish, in order to debug. If your data is correctly formatted, the system will respond with an **OK**, **NOTAUTHED**, **ERROR** or **REJECTED** as selected below. Alternatively you can select Random to have one of the four results randomly returned.

Authorisation Results	
You should code your site to send your VSP Direct authorisation request POSTs to: <b>http://ELEKTRA/VSPSimulator/VSPDirectGateway.asp</b>	
How would you like VSP Simulator to respond to your authorisation POSTs?	
<input checked="" type="radio"/> Random	VSP Simulator will act exactly like VSP Direct, validating your authorisation request POST to ensure the information you are sending is correct. If you have missed important fields, or formatted the POST badly a <b>MALFORMED</b> message will be sent back along with an explanation of the error in the <b>StatusDetail</b> field.  If you have send badly formatted or incorrect data in any of the fields you'll receive an <b>INVALID</b> message with an explanation of the error in the <b>StatusDetail</b> field.  If everything is formatted correctly and is validated successfully the system will send either an <b>OK</b> (60% of the time), <b>NOTAUTHED</b> (25%), <b>REJECTED</b> (10%) or <b>ERROR</b> (5%) to Simulate Live transactions.
<input type="radio"/> OK	VSP Simulator will validate your data in the same manner as Random mode above, but if the POST is validated successfully, an <b>OK</b> message will always be returned.
<input type="radio"/> MALFORMED	VSP Simulator will ALWAYS send a <b>MALFORMED</b> message, to allow you to test your error handling code.
<input type="radio"/> INVALID	VSP Simulator will ALWAYS send an <b>INVALID</b> message, to allow you to test your error handling code.
<input type="radio"/> ERROR	VSP Simulator will ALWAYS send an <b>ERROR</b> message, to allow you to test your error handling code.
<input type="radio"/> NOTAUTHED	VSP Simulator will validate your data in the same manner as Random mode above, but if the POST is validated successfully, a <b>NOTAUTHED</b> message will always be returned.
<input type="radio"/> REJECTED	VSP Simulator will validate your data in the same manner as Random mode above, but if the POST is validated successfully, a <b>REJECTED</b> message will always be returned.

Results of AVS and CV2 Checks	
Use the Radio buttons below to select the AVS and CV2 results you wish to see returned. In Random mode, the values are returned <b>MATCHED</b> (60%), <b>NOTMATCHED</b> (30%) and <b>NOTCHECKED</b> (10%). <b>NOTPROVIDED</b> is ALWAYS returned if you do not provide the Address, Postcode or CV2 information, but you can force that value to be returned if you wish to test your code.	
Address Check Result:	<input type="radio"/> NOTPROVIDED <input type="radio"/> NOTCHECKED <input type="radio"/> NOTMATCHED <input type="radio"/> MATCHED <input checked="" type="radio"/> Random
Post Code Check Result:	<input type="radio"/> NOTPROVIDED <input type="radio"/> NOTCHECKED <input type="radio"/> NOTMATCHED <input type="radio"/> MATCHED <input checked="" type="radio"/> Random
CV2 Check Result:	<input type="radio"/> NOTPROVIDED <input type="radio"/> NOTCHECKED <input type="radio"/> NOTMATCHED <input type="radio"/> MATCHED <input checked="" type="radio"/> Random

[Update](#)

This page allows you to define the behaviour of the VSP Simulator when it responds to your transaction registrations. By default the system will verify your POST to ensure the contents are correctly formatted and if they are, return a Random Status, along with all relevant fields (StatusDetail, VPSTxID, SecurityKey and so on). If your POST is incorrectly formatted or contains bad data, it will respond with a Status of MALFORMED or INVALID and explain what was wrong in the StatusDetail field.

This setting is useful in the final stages of testing, but for now you should select **OK/REGISTERED**, to force the Simulator to always provide a TxAuthNo if your data is not MALFORMED or INVALID (or a REGISTERED if your transaction type is an AUTHENTICATE). You can switch it back to Random once you are certain your system can process a successful end-to-end transaction.

You can simulate **NOTAUTHED** responses from the bank, or **REJECTED** messages as if your rulebases were applied. By simulating these messages you can check your own pages respond to the customer in the correct manner. You can also force errors, even if the data in the POST is okay. This is useful when testing upgrades to your scripts and proofing your error handling routines.

For now, select the **OK** setting, update the details, then log out of VSP Simulator.





## 3: Registering a Payment

If you don't plan to implement the protocol entirely on your own, you should install the most appropriate integration kit or worked example for your platform. These can be downloaded as part of the application process or obtained from the <http://techsupport.protx.com> downloads area.

The kits will not quite run out of the box because you have to provide some specific details about your site in the configuration files before a transaction can occur, but they will provide end of end examples of registering the transactions and handling the notification POSTs. Ensure you've completed all configuration in the includes file as detailed in the kit instructions, then locate the Transaction Registration script (normally called transactionRegistration).

This script provides a worked example of how to construct the transaction registration POST (see Appendix A section A1 in the attached protocol) and how to read the response that comes back (section A2).

If you plan to implement 3D-Secure Authentication, the kit also provides a Terminal URL example page which implements section A3 of the attached protocol.

Check that the payment registration script is sending transactions to the VSP Simulator (rather than the test or live sites) then execute this script. You may need to develop a simple payment page that allows you to enter card details and passes them to this script if this page is not included in your kit. Use the script to send a payment registration to the Simulator. You may wish to modify the script at this stage to echo the results of the POST to the screen, or a file, so you can examine the Status and StatusDetail reply fields to check for errors.

Once your script can successfully register a Payment and you receive a **Status** of **OK**, you should ensure your code stores the **VPSTxId**, **SecurityKey** and **TxAuthNo** fields alongside your uniquely generated **VendorTxCode** and the order details in your own database. You may wish to store the **3DSecureStatus** field if you plan to support 3D-Secure.

Your script should then redirect the customer to a completion page thanking them for their order.

In the real world, the bank will either authorise the transaction (an **OK** response) or fail it (a **NOTAUTHED** response), or Protx may reverse an authorisation if your fraud screening rules are not met (a **REJECTED** response). You should log into VSP Simulator in a separate browser window and change the response type to each of the failure messages in turn so you can write code to handle each message appropriately. Normally NOTAUTHED messages would prompt the user to try another card and REJECTED messages would ask them to check their Address and CV2 details are correct and resubmit, or to try another card. You may wish to store the VPSTxID and SecurityKey of the failed transaction against your VendorTxCode and generate a new VendorTxCode for the retry attempt if you wish to keep a history of the failed transactions as well as the successful ones.

# VSP Direct Protocol and Integration Guidelines



You should then use VSP Simulator to send each type of error message (MALFORMED, INVALID and ERROR) to your payment script to check that all message types are handled correctly. **MALFORMED** message should only occur during development when the POST may be incorrectly formatted, and **INVALID** messages can be avoided by pre-validating the user input. In the case of **ERROR**, your code should present the customer with a page saying that online payment was not currently available and offering them an alternative contact telephone number for payment or request them to come back later.

Once your page can handle every type of message returned by VSP Simulator, you should set the VSP Simulator to Random mode and attach the payment pages onto the end of your e-commerce site to test end-to-end transactions through your site. The Random mode will respond with an OK message 60% of the time, a NOTAUTHED 25% of the time, REJECTED 10% and ERROR 5% to allow you to ensure you site respond correctly in each circumstance.



## 4: 3D-Authenticated Transactions

If you plan to support the Verified by Visa and MasterCard SecureCode, collectively the 3D-Secure authentication system, you should go now go on to test that your scripts can handle these messages. You should ONLY do this once your transaction registration script can successfully process non-authenticated transactions as described in section 3 above.

Log into VSP Simulator, bring up the VSP Direct configuration page and select 3DAUTH as the response. Click the Update button.

Send a transaction registration POST to the VSP Simulator and rather than receiving an OK status, your script will receive a **3DAUTH** Status instead. A simulated **MD**, **PAReq** and **ACSURL** will be provided and you should ensure that your script builds the simple, automatically-submitting, HTML FORM code (as described in the step by step transaction process earlier in this document) and redirects your browser to the simulated 3D-Authentication page.

**Example Customer 3D-Authentication Page**

At this stage in the payment process you have successfully registered a VSP Direct 3D-Authenticated transaction and redirected your customer to their Card Issuing bank to complete their authentication. They will be presented with a screen like the one below.

**Merchant:** PROTX  
**Amount:** 15.23 GBP  
**Date:** 01/08/2006 11:35:53  
**Account:** XXXX XXXX XXXX 0001  
**Personal Message:** Welcome back 'Customer Name'  
**Password:**

**3D Notification to send to the Terminal URL**

Clicking one of the buttons below will format a 3D-Secure PAReq message and POST it to your **Terminal URL**. The page on your site pointed to by the Terminal URL should POST this information to the VSPDirect 3D Callback page.

This page will simulate the 3D completion and VSP Direct authorisation. Both **OK** and **ATTEMPTONLY** will return an authorised transaction, the other buttons return VSP Direct error messages of the selected type, to allow you to test your TerminalURL error handling code.

The **TermURL** field from your post is pointing to the following page:  
<https://margarine.protx.com/VSPDirect3DKit/CallBack.asp>

Ensure this is the correct URL for the Terminal URL on your site before clicking the buttons.

The <b>OK</b> response is sent when a transaction is successfully 3D-Secure Authenticated. Full liability shift occurs for transactions of this type.	<input type="button" value="OK"/>
This will cause VSP Simulator to simulate an authorised transaction. Your Terminal URL code should store the <b>VPSTxID</b> , <b>SecurityKey</b> , <b>TxAuthNo</b> & <b>CAVV</b> fields sent back against the transaction details in your database then direct your customer to an order completion page.	<input type="button" value="ATTEMPTONLY"/>
The <b>ATTEMPTONLY</b> response is sent by 3D-Secure if an attempt was made to authenticate but the process could not complete due to card issuer problems. Liability shift still occurs for Visa cards in this circumstance, but NOT MasterCard.	<input type="button" value="NOTAUTHED"/>
This will cause VSP Simulator to simulate an authorised transaction. Your Terminal URL code should store the <b>VPSTxID</b> , <b>SecurityKey</b> , <b>TxAuthNo</b> & <b>CAVV</b> fields sent back against the transaction details in your database then direct your customer to an order completion page.	<input type="button" value="REJECTED"/>
The <b>NOTAUTHED</b> message is sent when the user clicks aborts the 3D-Secure process or enters incorrect details into their Issuing Bank's system. This is a 3D-Secure failure.	<input type="button" value="ERROR"/>
The Simulator will adopt the default VSP System behaviour, which is to reject this message with a NOTAUTHED Status from VSPDirect. Your system should store the <b>VPSTxID</b> and <b>SecurityKey</b> in your database and redirect your customer to an order failure page.	<input type="button" value="MALFORMED"/>
The <b>REJECTED</b> message is sent by VSP Direct if the response from the 3D-Secure system failed your predefined rulebase.	<input type="button" value="INVALID"/>
Your Terminal URL code should store the <b>VPSTxID</b> and <b>SecurityKey</b> in your database and redirect the user to an order failure page.	
The <b>ERROR</b> , <b>MALFORMED</b> and <b>INVALID</b> messages are only sent if the 3D-Secure process goes wrong. Depending on your rulebase, VSP Direct will either reject this transaction (see Rejected above) or go on to obtain an authorisation which is NOT 3D-Secure. This simulator will return a VSP Direct Status of NOTAUTHED for these selections, with a <b>3DSecureStatus</b> set to the selected value.	
Note that in the Live environment, these transactions could be authorised. If you do not wish them to be, you will need to set up a rulebase to reject these 3D-Secure statuses.	
Since the Simulator returns a NOTAUTHED status, your Terminal URL code should store the <b>VPSTxID</b> and <b>SecurityKey</b> in your database and redirect the user to an order failure page.	

# VSP Direct Protocol and Integration Guidelines



This page displays the Terminal URL you have provided, and you should check that this points to the fully qualified URL of the Callback page provided in your kit. This should begin with https:// (since the Terminal URL should be secure) and provide the full path to the page.

If the URL is correct, you can select one of the buttons to create a Simulated **PARes** message that, when forwarded by your Terminal URL code to the VSP Simulator 3D callback page, will generate the VSP Direct result of your choosing.

Your Terminal URL code (normally a page called threeDCallback in the kits) should be modified to store the result fields in your database (as you did for your transaction registration code in section 3 above), including the **3DSecureStatus** field and, for 3D-Authenticated transactions, the **CAVV** field (the unique signature for a validated 3D-Secure transaction).

You can then direct your customer to the relevant completion page, depending on the Status of the transaction. Like non-authenticated transactions, a status of OK should redirect the user to a success page, and ERROR, NOTAUTHED, REJECTED, MALFORMED or INVALID to various error handling pages.

## 5: Examining your transactions

The VSP Simulator keeps the last month's worth of simulated transactions online for you to examine at your leisure. Using the Transactions button you can view everything you've sent us to ensure the data is as you expected.

The screenshot displays the VSP Simulator interface for 'Tony's Toupees'. It includes a 'Transaction List' section with a table of payments and a 'VSP Simulator Transaction Details' section showing specific transaction information.

**Transaction List**

VSP VendorTXCode	Received	Amount	VPS AuthCode	Status	Rep	Ref
Test713512599	23/02/05 10:09:36	40.00 (GBP)	0	Transaction registered and user successfully redirected to the payment pages.	X	X
Test791668117	23/02/05 10:05:30	40.00 (GBP)	0	Transaction registered and user successfully redirected to the payment pages.	X	X
<b>GBP Total:</b>		<b>80.00 (GBP)</b>				

**VSP Simulator Transaction Details**

**PAYMENT transaction.**

**Transaction Information**

Vendor TX Code:	Test713512599
VPSTxID:	(CF40EAD5-4811-4014-878D-91CEAFE14E9)
Security Key:	2103303L21
Status:	Transaction registered and user successfully redirected to the payment pages.
Description:	Some4thFromProts
Amount:	40.00 (GBP)
System Used:	VSP Server
Authorized:	Yes
VPS Auth Code:	0
Started:	23 February 2005 at 10:09:36
Refunded:	No
Repeated:	No
User:	VSP Simulator
Gift Add:	No
Notification URL:	http://192.168.0.142/ASPServer/VP3HandlePROTXResponse.asp

**Customer Details**

Customer Name:	
Client IP:	213.52.206.220

**Fraud Screening Information**

CV2 Values:	Not Provided
Post Code Values:	Not Provided
Address Numerics:	Not Provided
Checks Performed By:	Not known

You can also see from this screen which transactions have been subsequently refunded or used as the basis for repeat payments (see 6 below).

Once your site can handle all VSP Direct status types, on both your transaction registration and 3D-Secure Terminal URL pages, then you've completed your basic VSP Direct integration and can move on to testing your site against the real VSP Direct, firstly on the Test Server (see the next main section). If, however, you wish



to link in additional processes, such as Refunds or Repeats, or the ability to Release or Abort Deferred transactions, you should continue with step 6 below.

## 6: Additional Transaction Types

ProtX support a number of methods of registering a transaction and completing the payment.

### **DEFERRED transactions.**

By default a PAYMENT transaction type is used in your scripts to gain an authorisation from the bank, then settle that transaction early the following morning, committing the funds to be taken from your customer's card.

In some cases you may not wish to take the funds from the card immediately, but merely place a "shadow" on their card to ensure they cannot subsequently spend those funds elsewhere, and then only take the money when you are ready to ship the goods. This type of transaction is called a **DEFERRED** transaction and is registered in exactly the same way as a normal PAYMENT. You just need to change your script to send a TxType of DEFERRED when you register the transaction (protocol A1) instead of PAYMENT.

DEFERRED transactions are NOT sent to the bank for completion the following morning. In fact, they are not sent at all until you **RELEASE** them, either by sending a **RELEASE** message to our servers from yours (see the "VSP Server and Direct Shared Protocols" document for details on how to send this message) or by logging into the VSP Admin interface, finding the transaction and clicking the Release button.

If you are unable to fulfil the order, you can also **ABORT** deferred transactions in a similar manner and the customer will never be charged.

DEFERRED transactions work well in situations where it is only a matter of days between the customer ordering and you being ready to ship. Ideally all DEFERRED transaction should be released within 6 days (according to card scheme rules). After that the shadow may disappear from the card before you settle the transaction, you will have no guarantee that you'll receive the funds if the user has maxed out their card in the mean time. If you regularly require longer than 6 days to fulfil orders, you should consider using AUTHENTICATE and AUTHORISE instead of DEFERRED payments (see below)

DEFERRED transactions remain available for **RELEASE** for up to 30 days. After that time they are automatically **ABORTed** by the ProtX systems.





## REPEAT payments

If you have already successfully authorised a customer's card using as PAYMENT, a released DEFERRED or an AUTHORISE (see below) you can charge an additional amount to that card using the REPEAT transaction type, without the need to store the card details yourself.

If you wish to regularly REPEAT payments, for example for monthly subscriptions, you should ensure you have a "Continuous Authority" merchant number from your bank (please contact your acquiring bank for further details), but ad-hoc REPEATs do not require them. REPEAT payments cannot be 3D-Secured, or have CV2 checks performed on them (since ProtX are not allowed to store these values) so you are better to make use of Authenticate and Authorise if you need to vary the transaction amount on a regular basis.

## AUTHENTICATE and AUTHORISE

The AUTHENTICATE and AUTHORISE methods are specifically for use by merchants who are either (i) unable to fulfil the majority of orders in less than 6 days (or sometimes need to fulfil them after 30 days) or (ii) do not know the exact amount of the transaction at the time the order is placed (for example, items shipped priced by weight, or items affected by foreign exchange rates).

Unlike normal PAYMENT or DEFERRED transactions, AUTHENTICATE transactions do not obtain an authorisation at the time the order is placed. Instead the card and card holder are validated using the 3D-Secure mechanism provided by the card-schemes and card issuing banks.

Your site will register your transaction with a TxType of AUTHENTICATE. VSP Direct will contact the 3D-Secure directories to check if the card is part of the scheme. If it is not, then the card details are simply held safely at ProtX VSP Direct will reply with a Status of **REGISTERED** (This also happens if you do not have 3D-Secure active on your account or have used the Apply3DSecure flag to turn it off for that transaction).

If, however, the card *is* part of the 3D-Secure scheme, VSP Direct will reply with a Status of **3DAUTH** along with the MD, PAREq and ACSURL. You must then redirect the customer to their card issuing bank for authentication (just like a normal 3D-Secure payment, see steps 5 and 6 in the Payment Process above). Here they will authenticate themselves and be returned to your TermURL along with the PAREs and MD. These you'll forward to the VSP Direct 3D Callback page (as in step 7 above) and ProtX will decode the response for you.

If the customer has not passed authentication, your rule base is consulted to check if they can proceed for authorisation anyway. If not VSP Direct replies with a Status of **REJECTED**. If the customer failed authentication but can proceed, VSP Direct replies with a **REGISTERED** Status. If the user passed authentication with their bank and a CAVV/UCAF value is returned, your VSP Direct sends a Status of **AUTENTICATED** and a **CAVV** value for you to store if you wish.

In all cases, the customer's card is never authorised. There are no shadows placed on their account and your acquiring bank is not contacted. The customer's card details and their associated authentication status are simply held at ProtX for up to 90 days (a limit set by the card schemes, 30 days for International Maestro cards) awaiting an **AUTHORISE** or **CANCEL** request from your site (see the "VSP Server and Direct Shared Protocols" document for details of these messages).



To charge the customer when you are ready to fulfil the order, your site will need to send an **AUTHORISE** request. You can Authorise any amount up to 115% of the value of the Authentication and use any number of Authorise requests against an original Authentication so long as the total value of those authorisations does not exceed the 115% limit, and the requests are inside the 90 days limit. This is the stage at which your acquiring bank is contacted for an auth code. AVS/CV2 checks are performed at this stage and rules applied as normal. This allows you great flexibility for partial shipments or variable purchase values. If the AUTHENTICATE transaction was AUTHENTICATED (as opposed to simply REGISTERED) all authorisations will be fully 3D-Secured, so will still receive the fraud liability shift.

When you have completed all your Authorisations, or if you do not wish to take any, you can send a **CANCEL** message to VSP Server to archive away the Authentication and prevent any further Authorisations being made against the card. This happens automatically after 90 days.

Both AUTHORISE and CANCEL operations can also be performed in VSP Admin.

## REFUNDS and VOIDS

Once a PAYMENT, AUTHORISE or REPEAT transaction has been authorised, or a DEFERRED transaction has been RELEASEd, it will be settled with the acquiring bank early the next morning and the funds will be moved from the customer's card account, across to your merchant account. The bank will charge you for this process, the exact amount depending on the type of card and the details of your merchant agreement.

If you wish to cancel that payment before it is settled with the bank the following morning, you can send a **VOID** message to our servers to prevent the transaction ever being settled (see the "VSP Server and Direct Shared Protocols" document for more detail), thus saving you your transaction charges and the customer from ever being charged. You can also VOID transactions through the VSP Admin interface. VOIDed transactions can NEVER be reactivated though, so use this functionality carefully.

Once a transaction has been settled, however, you can no longer VOID it. If you wish to return funds to the customer you need to send a **REFUND** message to our servers, or use the VSP Admin screens to do the same.

You can REFUND any amount up to the value of the original transaction. You can even send multiple refunds for the same transaction so long as the total value of those refunds does not exceed the value of the original transaction. Again, the REFUND protocol can be found in the "VSP Server and Direct Shared Protocols" document.





## **VSP Simulator and Additional Transaction Types**

VSP Simulator can handle all the additional transaction types discussed above. It will accept PAYMENT, AUTHENTICATE and DEFERRED transactions at the registration stage, plus it has services that emulate those of the real VSP Server when you send REFUND, RELEASE, ABORT, REPEAT, AUTHORISE, CANCEL and VOID messages to it.

The additional transaction types, however, do not have a user configurable interface associated with them. By default they are all set to Automatic mode, so they will respond with an OK unless the data you send would generate a MALFORMED or INVALID response. Future versions of Simulator will extend this functionality to allow you to choose an appropriate response for each type of message.



## Stage 2: Testing on the Test Server

If your site works correctly against the VSP Simulator then this is normally a very quick step. The Test Server is an exact copy of the Live System but without the banks attached. This means you get a true user experience but without the fear of any money being taken from your cards during testing.

In order to test on the Test Server, however, you need a Test Server account to be set up for you by the Protix Support team. These accounts can **only** be set up once you have completed all sections of the Online Registration forms (<https://support.protix.com/apply>) including the Merchant Account section. Often when applying to trade online it takes a while for the Merchant Account to be assigned by your acquirer, so you may wish to ensure that you set those wheels in motion before you begin your integration with Protix, to ensure things don't bottleneck at this stage.

The Support Team will set up an account for you on the Test Server under the same VSP Vendor Name as your online application form and Simulator account. You will, however, be issued with different passwords for security purposes. The Support Team will let you know how to retrieve those passwords and from there how to use the VSP Admin screens to look at your transactions.

To link your site to the Test Server, you need only to change your transaction registration script to send the message to the Test Server URL for VSP Direct rather than the Simulator. In many kits this is done simply by change this Test Server flag in the configuration scripts to 1. If you've been developing your own scripts, then the Test Site URL for payment registration is:

<https://ukvpstest.protix.com/vspgateway/service/vspdirect-register.vsp>

(for other transaction types, the final vspdirect-register.vsp section would be changed to refund.vsp, release.vsp, void.vsp etc.)

You will always receive an OK message and an Authorisation Code from the test server if you are using one of the test cards listed below. All other valid card numbers will be declined, allowing you to test your failure pages. If you do not use the correct Address, Post Code and CV2 digits, the transaction will still authorise, but you will receive NOTMATCHED messages in the AVS/CV2 checks, allowing you to test your rule-bases and fraud specific code.

Card Type	Card Number	Issue	CV2	Address	PostCode
Visa Credit	4929 0000 0000 6		123	88	412
MasterCard Credit	5404 0000 0000 0001		123	88	412
Visa Debit / Delta	4462 0000 0000 0003		123	88	412
Solo	6334 9000 0000 0005	1	123	88	412
UK Maestro	5641 8200 0000 0005	01	123	88	412
American Express	3742 000000 00004		123	88	412
Visa Electron	4917 3000 0000 0008		123	88	412
JCB	3569 9900 0000 0009		123	88	412
Diner's Club	3600 0000 0000 08		123	88	412

# VSP Direct Protocol and Integration Guidelines



If you have 3D-Secure set up on your test account, you can use the VSP Admin interface to switch on the checks at this stage to test your 3D-Secure terminal URL script against a simulation of the 3D-Secure environment.

This simulation is more advanced than the VSP Simulator process because it creates real PaReq and PaRes messages. It does not talk to the real Visa and MasterCard systems though, so no live authentications can occur.

At the Simulated Authentication screens, to successfully authentication the transaction, enter "password" (without the quotes) into the password box. Any other phrase will fail the authentication, allowing you to test your rules and 3D-Secure response handling. We'll be extending this over the next few months to allow you to simulate all 3D-Secure responses.

At the 3D-secure callback stage you'll need to change your POST to go to:  
<https://ukvpstest.protx.com/vspgateway/service/direct3dcallback.vsp>

Once you've checked you can process an end-to-end transaction and, where appropriate, can successfully process 3D-Authentication, and tested any additional transaction types you have set up (such as Refunds and Releases) then you are almost ready to go live. Before doing so, however, you should log in to the Protx VSP Admin system on the test servers to view your transactions and familiarise yourself with the interface.



## The Test Server VSP Admin

A Test Server version of the VSP Admin system is available to you whilst using your test account to view your transactions, refund payments, release deferred payments, void transactions etc. You should familiarise yourself with this system on the Test Server before you go live so you know how to use the system in anger on the Live Servers.

The Test Server VSP Admin can be found at: <https://ukvpstest.protx.com/VSPAdmin>

Please note: You will need both JavaScript and Cookies enabled to view this site.  
Protx also recommend using Internet Explorer or Netscape versions 4 or above.  
If you are using an older browser version you should consider updating it for security reasons.

When you log in to the VSP Admin screens you will be asked for a **Vendor Name**, a **User Name** and a **Password**. The first time you log in you will need to do so as your system Administrator:

- In the **Vendor Name** box, enter your VSP Vendor Name, as selected in your Online Registration screens and used throughout the development as your unique merchant identifier.
- In the **User Name** box, enter the VSP Vendor Name **again**.
- In the **Password** box, enter the VSP Admin password as supplied to you by Protx when your test account was set up.
- Click **Login**.

User Name	Access Level	Logged In?	Locked Out?	Actions
Admin Account (protx)	<b>IMPORTANT!</b> The Administrative user can ONLY be used to create and manage other user accounts and change account permissions. You will need to create your own user (using the Add button below) before you can view transactions, reports or VSP Terminal.	Yes	No	You cannot change the System Admin account. Contact Protx if you need assistance.

Or to create a new User Account, click here: [Add](#)

# VSP Direct Protocol and Integration Guidelines



The administrator can ONLY create user accounts, unlock other accounts and change account parameters. You cannot, whilst logged in as administrator, view your transactions or take payments through the online terminal.

securing future e-commerce

Current Vendor: Protix Ltd  
Current User: protix

Logout Help

New Test Updates Administration

**Administrative Functions - Add New User**  
Enter the details of the new user below.  
You must specify at least one access area, a default home page and enter a password in BOTH boxes.  
Click the Add button to create the new user or Cancel to go back to the User Admin page.

**Enter New User Details**

User Name:   
Password:   
Confirm Password:

**Account Privileges**

☒ User can View System transactions and Other User's transactions as well as their own.  
☐ User can REFUND any Payment transaction they have access to.  
☒ User can RELEASE Deferred or RepeatDeferred Payments.  
☒ User can ABORT Deferred or RepeatDeferred Payments.  
☐ User can VOID ANY completed, authorised transaction not already submitted to the acquirer in a batch file.  
☐ User can make REPEAT or REPEATDEFERRED payments against a card used in any previously authorised transaction.

**VSP Admin Access**

☒ **Transactions** Allows access to Transaction Lists and Details. From the Detail screens, depending on the privileges set above, the user can REFUND, RELEASE, REPEAT and ABORT transactions.  
☒ **Reports** Allows access to the Report screens. Users limited to view only their own transactions will only be able to report on their own transactions.  
☒ **VSP Terminal** Allows access to the VSP Terminal screens to take new Payments.  
☐ **Updates** Allows access to the News and Updates pages from Protix.  
☐ **Administration** Allows access to the Admin pages (including this user section). Use discretion when granting this access.  
The page to which the user is directed when they first log in.  
NOTE: If users can see the Updates section they will ALWAYS be taken to the Updates page first whenever unread news or updates are present.

Transaction List

Cancel Add

To use those functions, and to protect the administrator account, you need to create new users for yourself and others. Click the Add button to add a new user.

Enter a username for yourself and a password you'll remember, then ensure all the check boxes are enabled for your account. Click the Add button and your new account will appear in the list.

Now click the Logout button and click to Log back in, this time entering:

- Your VSP Vendor name in the **Vendor Name** box.
- The User Name of the account you just created in the **User Name** box.
- The password for the 'user' account you just created in the **Password** box.

...and click **Login**.

You are now logged in using your own account and can view your test transactions and use all additional functions. You need only log in as Administrator again if you wish to create additional users, or if you lock yourself out of your own account, you can use the Administrator account to unlock yourself. If you happen to lock out the Administrator account, you will need to contact Protix to unlock it for you.

Detailed context sensitive help is available on every VSP Admin page by clicking the Help button, so a description of the functions will not be presented here. Play with the system until you are comfortable with it though, you cannot inadvertently charge anyone or damage anything whilst on the test server.



## Stage 3: Going Live

In order to go live all of the following criteria MUST be met:

- You have completed testing all your transaction types against the Test Server account.
- You have logged into the VSP Admin system on the Test Server, created a user for yourself and viewed and refunded some of your Test transactions as that user.
- You have completed the Online Direct Debit sign-up form to allow Protix to invoice you for services each month.

The Live Team cannot set your account up until all three actions have been completed.

When you have finished your testing and signed up ready to go, you need to send an e-mail to [golive@protix.com](mailto:golive@protix.com) with your VSP Vendor Name included in the mail. The Live Team will normally begin processing that request the same day, but it can take up to 24 hours in busy periods.

The amount of time it takes for your Live account to activate depends on your acquiring bank:

- Lloyds TSB, Bank of Scotland and American Express are active as soon as the Live Team upload your account.
- Barclays Merchant Service and Natwest Streamline require a 24-hour activation period.
- HSBC can take up to 72 hours to activate your account.

Where possible we set the wheels in motion as early as possible by requesting activation of your account at the stage we set up your Test Server account, but please be aware of these delays when sending your "Go Live" message. Don't send it on Friday if you need to be live on Saturday and bank with HSBC.

Once your Live account is active, you should point your web site transaction registration scripts at the following URL:

<https://ukvps.protix.com/vspgateway/service/vspdirect-register.vsp>

(for other transaction types, the vspdirect-register.vsp section would be changed to refund.vsp, void.vsp, release.vsp etc.)

The 3D-Secure callback URL becomes:

<https://ukvps.protix.com/vspgateway/service/direct3dcallback.vsp>

You should then run an end-to-end transaction through your site, ordering something relatively inexpensive from your site and paying using your own valid credit or debit card. If you receive an authorisation code, then everything is working correctly.

# VSP Direct Protocol and Integration Guidelines



Finally should then log into the Live Server VSP Admin screens at <https://ukvps.protx.com/VSPAdmin> and in a similar manner to the test server, first log in as the Administrator, then create a Live System user for yourself, log in as that user, locate your test transaction and VOID it, so you are not charged for the transaction. At this stage the process is complete.

It is worth noting here that none of the users you set up on the VSP Admin system on the Test Server are migrated across to Live. This is because many companies use third party web designers to help design the site and create users for them during test that they would not necessarily like them to have in a live environment. You will need to recreate any valid users on the Live system when you first log in.





## Congratulations, you are now Live with VSP Direct

Well done. Hopefully the process of getting here was as painless and hassle free as possible. You'll be pleased to know that now you are live we don't cut the strings and run away. You should contact us with any transaction queries that arise or for any help you need with the VSP Admin system.

Here are the best ways to reach us and the best people to reach:

- If you require any information on additional services, have a query regarding a Protx invoice, or have a general question about online payments or fraud, e-mail [info@protx.com](mailto:info@protx.com) with your VSP Vendor Name included with your question.
- If you have a question about a transaction, have issues with your settlement files or are having problems with your payment pages or VSP Admin screens, e-mail [support@protx.com](mailto:support@protx.com) with your VSP Vendor Name included in the mail.
- If you have any suggestions for future enhancements to the system, or additional functionality you'd like to see added, please mail [feedback@protx.com](mailto:feedback@protx.com) with your comments. We do take all comments on board when designing upgrades, although we may not be able to answer every mail we get.
- If you wish to be part of our Beta test program for future system upgrades, mail [beta@protx.com](mailto:beta@protx.com) and let us know your VSP Vendor Name so we can include you in the scheme.
- You can call us as well on 0845-111-4455, selecting option 1 for the Info team or 4 for the Support team, although our primary method of contact is via e-mail, especially for the Support team, who work on ticketed systems to ensure queries are answered in strict rotation. Lines into Support are limited so where possible it is better to e-mail.

We will also keep you updated about major system changes, new reports and other enhancements via the Updates section in VSP Admin, plus your e-mail address will be added to our group mail list used to alert you to upgrades and other pending events.

You can also always check our system availability and current issues on the VSP Monitor page at <http://www.protx.com/services/monitorvsp.asp>

Thanks again for choosing Protx, and we wish you every success in your e-commerce venture.



## Appendix A – The VSP Direct Protocol v2.22

This section details the contents of the POST sent to VSP Direct from your servers, quantifying the returned values where appropriate.

### A1: Transaction registration

This is performed via a **HTTPS POST** request, sent to the initial VSP Direct Payment URL. The details should be URL encoded Name=Value fields separated by '&' characters.

#### Request format (continued overleaf)

Name	Format	Values	Comments
VPSPProtocol	Alphanumeric. Fixed 4 characters.	"2.22" in this release	Default or incorrect value is taken to be 2.22.
TxType	Alphanumeric Max 15 characters.	"PAYMENT", "DEFERRED" or "AUTHENTICATE"	See companion document "VSP Server and Direct Shared Protocols" other transaction types (such as Refund, Releases, Aborts and Repeats).
Vendor	Alphanumeric Max 15 characters.	Vendor Login Name	Used to authenticate your site. This should contain the VSP Vendor Name supplied by ProtX when your account was created.
VendorTxCode	Alphanumeric Max 40 characters	Vendor Transaction Code	This should be your own reference code to the transaction. Your servers should provide a completely unique VendorTxCode for each transaction.
Amount	Numeric. 1.00 to 100,000.00	Amount for the Transaction containing minor digits formatted to 2 decimal places where appropriate.	Must be positive and numeric, and may include a decimal place where appropriate. Minor digits should be formatted to two decimal places. e.g. 5.10, or 3.29. Values such as 3.235 will be rejected.
Currency	Alphanumeric 3 characters	Three-letter currency code to ISO 4217 Examples: "GBP", "EUR" and "USD"	The currency must be supported by one of your VSP merchant accounts or the transaction will be rejected.
Description	Alphanumeric Max 100 characters	Free text description of goods or services being purchased	The description of good purchased is displayed in the Administrative screens for your future reference.
CardHolder	Alphanumeric Max 50 characters	The card holder's name	This should be the name displayed on the card.
CardNumber	Numeric Max 20 characters	The credit or debit card number with no spaces.	The full card number is required.
<b>Optional:</b> StartDate	Numeric 4 characters	The Start date (required for some Maestro, Solo and Amex) in <b>MMYY</b> format	The start date MUST be in MMYY format i.e. 0699 for June 1999. No / or – characters should be included.
ExpiryDate	Numeric 4 characters	The Expiry date (required for ALL cards) in <b>MMYY</b> format	The expiry date MUST be in MMYY format i.e. 1206 for December 2006. No / or – characters should be included.

# VSP Direct Protocol and Integration Guidelines



(continued overleaf)

<b>Optional:</b> IssueNumber	Numeric Max 2 characters	The card Issue Number (some Maestro and Solo cards only)	The issue number MUST be entered EXACTLY as it appears on the card. e.g. some cards have issue number "4" others have "04".
<b>Optional:</b> CV2	Numeric Max 4 characters	The extra security 3 digits on the signature strip of the card, or the extra 4 digits on the front for American Express Cards	<b>NB: If AVS/CV2 is ON for your account this field becomes compulsory.</b>
CardType	Alphanumeric Max 15 characters	"VISA", "MC", "DELTA", "SOLO", "MAESTRO", "UKE", "AMEX", "DC" or "JCB" NB: "SWITCH" is still accepted but you should use "MAESTRO"	MC is MasterCard, UKE is Visa Electron. AMEX and DC (DINERS) can only be accepted if you have additional merchant accounts with those acquirers.
<b>Optional:</b> BillingAddress	Alphanumeric Max 200 characters	The Card Holder's Billing Address (the address at which the card is registered) <b>WITHOUT</b> the Post/Zip code. (previous called <b>Address</b> )	<b>NB: If AVS/CV2 is ON for your account this field becomes compulsory.</b> Ensure the Post code is not included or Address Verification checks will fail.
<b>Optional:</b> BillingPostCode	Alphanumeric Max 10 characters	The Post/Zip code of the Card Holder's Billing Address (the address at which the card is registered). Previous called <b>PostCode</b> )	<b>NB: If AVS/CV2 is ON for your account this field becomes compulsory.</b>
<b>Optional:</b> DeliveryAddress	Alphanumeric Max 200 characters	Free format field for the customer's Delivery Address without the Post/Zip code	The information, whilst not used for authorisation purposes, IS used by our fraud screening partner
<b>Optional:</b> DeliveryPostCode	Alphanumeric Max 10 characters	The Post code or Zip code of the customer's delivery address	The information, whilst not used for authorisation purposes, IS used by our fraud screening partner
<b>Optional:</b> CustomerName	Alphanumeric Max 100 characters	The name of the customer.	This is the name of customer to whom the goods are ordered. This field is provided because it is not necessarily the same as the <b>CardHolder</b> name above (which is compulsory).
<b>Optional:</b> ContactNumber	Alphanumeric Max 20 characters	The telephone number on which to contact the customer.	The information, whilst not used for authorisation purposes, IS used by our fraud screening partner. You should request a land line where possible.
<b>Optional:</b> ContactFax	Alphanumeric Max 20 characters	The fax number on which to contact	The information is not used in customer validation at present and is available for reporting purposes only.
<b>Optional:</b> CustomerEMail	Alphanumeric Max 255 characters	The customer's e-mail address	The current version of VSP Direct does not send confirmation e-mails to the customer (although future versions will). This field is provided for your records only.
<b>Optional:</b> Basket	Alphanumeric Max 7500 characters	See the next section for the Format of the Basket field	You can use this field to supply details of the customer's order. This information will be displayed to you in the VSP Admin screens.

# VSP Direct Protocol and Integration Guidelines



<b>Optional:</b> GiftAidPayment	Flag	<p><b>0</b> = This transaction is not a Gift Aid charitable donation (default)</p> <p><b>1</b> = This payment is a Gift Aid charitable donation and the customer has AGREED to donate the tax.</p>	Only of use if your vendor account is Gift Aid enabled. Setting this field means the customer has ticked a box on your site to indicate they wish to donate the tax. See Gift Aid rules for more details.
<b>Optional:</b> ApplyAVSCV2	Flag	<p><b>0</b> = If AVS/CV2 enabled then check them. If rules apply, use rules. (default)</p> <p><b>1</b> = Force AVS/CV2 checks even if not enabled for the account. If rules apply, use rules.</p> <p><b>2</b> = Force NO AVS/CV2 checks even if enabled on account.</p> <p><b>3</b> = Force AVS/CV2 checks even if not enabled for the account but DON'T apply any rules.</p>	Using this flag you can fine tune the AVS/CV2 checks and rule set you've defined at a transaction level. This is useful in circumstances where direct and trusted customer contact has been established and you wish to override the default security checks.
<b>Optional:</b> ClientIPAddress	Alphanumeric Max 15 characters	The IP address of the client connecting to your server making the payment.	This should be a full IP address which you can obtain from your server scripts. We will attempt to Geolocate the IP address in your reports and fraud screening.
<b>Optional (3D-Secure only):</b> Apply3DSecure	Flag	<p><b>0</b> = If 3D-Secure checks are possible and rules allow, perform the checks and apply the authorisation rules. (default)</p> <p><b>1</b> = Force 3D-Secure checks for this transaction only (if your account is 3D-enabled) and apply rules for authorisation.</p> <p><b>2</b> = Do not perform 3D-Secure checks for this transaction only and always authorise.</p> <p><b>3</b> = Force 3D-Secure checks for this transaction (if your account is 3D-enabled) but ALWAYS obtain an auth code, irrespective of rule base.</p>	Using this flag you can fine tune the 3D Secure checks and rule set you've defined, at a transaction level. This is useful in circumstances where direct and trusted customer contact has been established and you wish to override the default security checks.
<b>Optional:</b> AccountType	Alphanumeric 1 character	<p><b>E</b> = Use the e-commerce merchant account. (default)</p> <p><b>C</b> = Use the continuous authority merchant account (if present).</p> <p><b>M</b> = Use the mail order, telephone order account (if present).</p>	This optional flag is used to tell the VSP System which merchant account to use for this transaction in situations where more than one type of merchant account is set up for your Protix vendor account. If omitted, the system will use E, then M then C by default.



## Basket Contents

The shopping basket contents can be passed in a single, colon-delimited field, in the following format:

```
Number of lines of detail in the basket field:
Item 1 Description:
Quantity of item 1:
Unit cost item 1 without tax:
Tax applied to item 1:
Cost of Item 1 including tax:
Total cost of item 1 (Quantity x cost including tax):
Item 2 Description:
Quantity of item 2:
....
Cost of Item n including tax:
Total cost of item n
```

## IMPORTANT NOTES:

- (i) The line breaks above are included for readability only. No line breaks should be included; the only separators should be the colons.
- (ii) The first value "The number of lines of detail in the basket" is **NOT** the total number of items ordered, but the total number of rows of basket information. In the example below there are 6 items ordered, (1 DVD player and 5 DVDs) but the number of lines of detail is 4 (the DVD player, two lines of DVDs and one line for delivery)

So, for example, the following shopping cart...

Items	Quantity	Item value	Item Tax	Item Total	Line Total
Pioneer NSDV99 DVD-Surround Sound System	1	£424.68	£74.32	£499.00	£499.00
Donnie Darko Director's Cut	3	£11.91	£2.08	£13.99	£41.97
Finding Nemo	2	£11.05	£1.94	£12.99	£25.98
Delivery	---	---	---	---	£4.99

Would be represented thus:

```
4:Pioneer NSDV99 DVD-Surround Sound System:1:£424.68:£74.32:£499.00:
£499.00:Donnie Darko Director's Cut:3:£11.91:£2.08:£13.99:£41.97:
Finding Nemo:2:£11.05:£1.94:£12.99:£25.98: Delivery:---:---:---:
---:£4.99
```

If you wish to leave a field empty, you must still include the colon. e.g.

```
DVD Player:1:£199.99::£199.99
```



## A2: Protx Response to the Transaction Registration or Callback POSTs

This is the plain text response part of the POST originated by your servers in A1. Encoding will be as Name=Value fields separated by carriage-return-linefeeds (CRLF).

### Response format (continued overleaf):

Name	Format	Values	Comments
VSPProtocol	Alphanumeric. Fixed 4 characters.	Version number of the protocol of the system. This release will return "2.22"	This will match the protocol version supplied in A1.
Status	Alphanumeric Max 15 characters.	<p>"OK" – The transaction was authorised by the bank and funds have been taken from the customer.</p> <p>"MALFORMED" – Input message was missing fields or badly formatted – normally will only occur during development and vendor integration.</p> <p>"INVALID" – Transaction was not registered because although the POST format was valid, some information supplied was invalid. E.g. incorrect vendor name or currency.</p> <p>"NOTAUTHED" – The transaction was not authorised by the acquiring bank. No funds could be taken from the card.</p> <p>"REJECTED" – The VSP System rejected the transaction because of the rules you have set on your account.</p> <p>"3DAUTH" – The customer needs to be directed to their card issuer for 3D-Authentication.</p> <p>"AUTHENTICATED" – The 3D-Secure checks were performed successfully and the card details secured at Protx.</p> <p>"REGISTERED" – 3D-Secure checks failed or were not performed, but the card details are still secured at Protx.</p> <p>"ERROR" – An error occurred at Protx which meant the transaction could not be completed successfully.</p>	<p>If the status is not <b>OK</b>, the <b>StatusDetail</b> field will give more information about the status.</p> <p>Please notify Protx if a Status report of <b>ERROR</b> is seen, together with your VendorTxCode and the StatusDetail text.</p> <p><b>3DAUTH</b> is only returned if 3D-Authentication is available on your account AND the card and card issuer are part of the scheme. A Status of 3DAUTH only returns the StatusDetail, MD, PAREq, 3DSecureStatus and ACSURL fields. The other fields are returned with other Status codes only.</p> <p><b>AUTHENTICATED</b> and <b>REGISTERED</b> statuses are only returned if the TxType is <b>AUTHENTICATE</b>.</p>
StatusDetail	Alphanumeric Max 255 characters	Human-readable text providing extra detail for the Status message.	Always check StatusDetail if the Status is not <b>OK</b>
VPSTxId	Alphanumeric 38 characters	Protx ID to uniquely identify the Transaction on our system.	<p>You should store this value and quote it to us if you have a query about the transaction.</p> <p>Not present when Status is <b>3DAUTH</b>.</p>
SecurityKey	Alphanumeric 10 characters	Security key which VSP uses to generate an MD5 Hash to sign the transaction.	<p>Should be kept secret from the Customer but stored in your database.</p> <p>Not present when Status is <b>3DAUTH</b>.</p>
TxAuthNo	Numeric Long integer	The Protx authorisation code (also called <b>VPSAuthCode</b> ) for this transaction.	Only present if Status is <b>OK</b> .

# VSP Direct Protocol and Integration Guidelines



(continued overleaf)

AVSCV2	Alphanumeric Max 50 characters	Response from AVS and CV2 checks. Will be one of the following: <b>"ALL MATCH"</b> , <b>"SECURITY CODE MATCH ONLY"</b> , <b>"ADDRESS MATCH ONLY"</b> , <b>"NO DATA MATCHES"</b> or <b>"DATA NOT CHECKED"</b> .	Provided for Vendor info and backward compatibility with the banks. Rules set up at the VSP server will accept or reject the transaction based on these values. More detailed results are split out in the next three fields. Not present if the Status is <b>3DAUTH, AUTHENTICATED</b> or <b>REGISTERED</b> .
AddressResult	Alphanumeric Max 20 characters	<b>"NOTPROVIDED"</b> , <b>"NOTCHECKED"</b> , <b>"MATCHED"</b> , <b>"NOTMATCHED"</b>	The specific result of the checks on the cardholder's address numeric from the AVS/CV2 checks. Not present if the Status is <b>3DAUTH, AUTHENTICATED</b> or <b>REGISTERED</b> .
PostCodeResult	Alphanumeric Max 20 characters	<b>"NOTPROVIDED"</b> , <b>"NOTCHECKED"</b> , <b>"MATCHED"</b> , <b>"NOTMATCHED"</b>	The specific result of the checks on the cardholder's Post Code from the AVS/CV2 checks. Not present if the Status is <b>3DAUTH, AUTHENTICATED</b> or <b>REGISTERED</b> .
CV2Result	Alphanumeric Max 20 characters	<b>"NOTPROVIDED"</b> , <b>"NOTCHECKED"</b> , <b>"MATCHED"</b> , <b>"NOTMATCHED"</b>	The specific result of the checks on the cardholder's CV2 code from the AVS/CV2 checks. Not present if the Status is <b>3DAUTH, AUTHENTICATED</b> or <b>REGISTERED</b> .
3DSecureStatus	Alphanumeric Max 20 characters	<p><b>"OK"</b> – The 3D-Authentication step completed successfully. If the Status field is 3DAUTH, this means the card is part of the scheme. If the Status field is OK too, then this indicates that the authorized transaction was also 3D-authenticated and a CAVV will be returned. Liability shift occurs.</p> <p><b>"NOAUTH"</b> – Returned with a Status of 3DAUTH. This means the card is not in the 3D-Secure scheme.</p> <p><b>"CANTAUTH"</b> - Returned with a Status of 3DAUTH. This normally means the card Issuer is not part of the scheme.</p> <p><b>"NOTAUTHED"</b> – The cardholder failed to authenticate themselves with their Issuing Bank.</p> <p><b>"ATTEMPTONLY"</b> – The cardholder attempted to authenticate themselves but the process did not complete. A CAVV is returned anyway and liability shift occurs for non-Maestro cards. Check VSP Admin.</p> <p><b>"NOTCHECKED"</b> - No 3D Authentication was attempted for this transaction. Always returned if 3D-Secure is not active on your account.</p> <p><b>"MALFORMED"</b>, <b>"INVALID"</b>, <b>"ERROR"</b> – These statuses indicate a problem with creating or receiving the 3D-Secure data. These should not occur on the live environment.</p>	<p>This field holds the results of the 3D-Authentication steps carried out by VSP Direct and the ProtX MPI.</p> <p>If 3D-Secure is not active on your account, this field will always contain the value <b>NOTCHECKED</b>.</p>



# VSP Direct Protocol and Integration Guidelines



CAVV	Alphanumeric Max 32 characters	The encoded result code from the 3D-Secure checks. Holds the Visa CAVV or the MasterCard UCAF depending on the card type used in the transaction.	Only present if the 3DSecureStatus field is <b>OK</b> AND the Status field is <b>OK</b>
MD	Alphanumeric Max 35 characters	A unique reference for the 3D-Authentication attempt.	Only present if the Status field is <b>3DAUTH</b> .
ACSURL	Alphanumeric Max Unlimited, but practical limit should be 7,500 characters	A fully qualified URL that points to the 3D-Authentication system at the Cardholder's Issuing Bank.	Only present if the Status field is <b>3DAUTH</b> .
PAReq	Alphanumeric Max Unlimited, but practical limit should be 7,500 characters	A Base64 encoded, encrypted message to be passed to the Issuing Bank as part of the 3D-Authentication.	Only present if the Status field is <b>3DAUTH</b> .  NOTE: When forwarding this value to the ACSURL, pass it in a field called <b>PaReq</b> (note the lower case a). This avoids issues with case sensitive ACSURL code.



## A3: 3D-Authentication Results POST from your Terminal URL to Protx.

This is performed via a **HTTPS POST** request, sent to the VSP Direct 3D Callback URL. The details should be URL encoded Name=Value fields separated by '&' characters.

### Request format

Name	Format	Values	Comments
MD	Alphanumeric Max 35 characters	A unique reference for the 3D-Authentication attempt.	This will match the MD value passed back to your site in response to your transaction registration POST.
PARes	Alphanumeric Max Unlimited, but practical limit should be 7,500 characters	A Base64 encoded, encrypted message sent back by Issuing Bank to your Terminal URL at the end of the 3D-Authentication process.	This field must be passed back to VSP Direct along with the MD field to allow the Protx MPI to decode the result.

## A4: Response to 3D Callback POSTs

The response from the 3D callback is identical to that of the initial registration POST. See section A2 above.

## A5: VSP Direct Full URL Summary

The table below shows the complete web addresses to which you send the messages detailed above.

Transaction Registration (PAYMENT, DEFERRED, AUTHENTICATE)	
<b>VSP Simulator:</b>	<a href="https://ukvpstest.protx.com/VSPSimulator/VSPDirectGateway.asp">https://ukvpstest.protx.com/VSPSimulator/VSPDirectGateway.asp</a>
<b>TEST System:</b>	<a href="https://ukvpstest.protx.com/vspgateway/service/vspdirect-register.vsp">https://ukvpstest.protx.com/vspgateway/service/vspdirect-register.vsp</a>
<b>Live System:</b>	<a href="https://ukvps.protx.com/vspgateway/service/vspdirect-register.vsp">https://ukvps.protx.com/vspgateway/service/vspdirect-register.vsp</a>

3D-Secure Callback	
<b>VSP Simulator:</b>	<a href="https://ukvpstest.protx.com/VSPSimulator/VSPDirectCallback.asp">https://ukvpstest.protx.com/VSPSimulator/VSPDirectCallback.asp</a>
<b>TEST System:</b>	<a href="https://ukvpstest.protx.com/vspgateway/service/direct3dcallback.vsp">https://ukvpstest.protx.com/vspgateway/service/direct3dcallback.vsp</a>
<b>Live System:</b>	<a href="https://ukvps.protx.com/vspgateway/service/direct3dcallback.vsp">https://ukvps.protx.com/vspgateway/service/direct3dcallback.vsp</a>