



VSP Form Protocol and Integration Guidelines



Document Index

Welcome to VSP Form.....	3
Overview of how VSP Form Payments work	4
The VSP Form Payment Process in Detail	5
Step 1: The customer orders from your site.	5
Step 2: Your server builds a Confirmation Page.....	5
Step 3: Customer enters card details on VSP Form.	6
Step 4: VSP Form requests card authorisation.	7
Step 5: VSP Form Redirects the Customer to your site.	8
Step 6: VSP sends daily Batch File to confirm payments.	9
Integrating with VSP Form.....	10
Stage 1: Integrating with the VSP Simulator	11
1: VSP Simulator Account Set up	12
2: Registering a Payment.....	13
3: Examining your transactions	15
4: Additional Transaction Types	16
Stage 2: Testing on the Test Server	18
The Test Server VSP Admin.....	19
Stage 3: Going Live	21
Congratulations, you are now Live with VSP Form	22
Appendix A - The VSP Form Protocol v2.22	23
A1: Transaction registration	23
A2: Transaction Completion	27



Welcome to VSP Form

The PROTX Veri-Secure Payment system (VSP) provides a secure, simple means of authorising credit and debit card payments and refunds, on your web site.

The VSP system provides a straightforward payment interface for the customer, and takes complete responsibility for the online transaction, including the collection and encrypted storage of credit/debit card details, eliminating the security implications of holding such sensitive information on your own servers.

VSP Form is designed for merchants who use shopping carts, have less experience in server side scripting, or who use shared web servers that do not offer database services. With VSP Form, all transaction information is held at Protix, including the full shopping basket contents, and e-mails are sent from the Protix servers to you and your customers to confirm the success or failure of the transaction.

The customer is redirected to Protix to enter their card details, so no sensitive information needs to be taken or stored on your site (removing the need for you to maintain highly secure encrypted databases, or obtain digital certificates).

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

PLEASE NOTE: Originally the PROTX VSP Form 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 and have remained unchanged because the protocols have been extended rather than replaced.



Overview of how VSP Form Payments work

The final “Pay Now” button on your website is your link to the PROTX VSP System. Once the customer has selected their purchases, entered delivery details, billing address and so forth, all on your own site, and pressed the final proceed button, a small script on your server generates an order summary page, listing the customer’s contact details, their purchases and the total order amount. At the bottom of that page is a “Pay Now” button which submits the information on that page to the VSP Form gateway.

What the customer doesn’t see is that whilst generating that order summary page, a simple and easy to modify piece of server-side scripting builds an encrypted hidden field that it places on the form. This field contains all the transaction information in a format that VSP Form can understand. When the user clicks the “Pay Now” button, the encrypted contents of that field get POSTed to VSP Form and the customer is presented with the Protix payment pages, where they enter their credit/debit card details, security codes and billing address (if you have not already captured it). The VSP Form main page carries your logo, and a description of the goods the customer is paying for, so they can remain confident they are buying from you. You can even customise those payment pages to carry the look and feel of your site at no additional cost.

Once the customer has selected their payment method and confirmed they really wish to complete the payment, VSP Form requests authorisation from your acquiring bank. Once the bank has authorised the payment (and assuming the address and card value checks have passed any rules you may have set up), we redirect your customer back to the successful payment page on your site. If the authorisation fails, we redirect the customer to your order failure page. Both pages are sent encrypted information which you can decrypt, again using simple scripts, to find out what happened to the transaction and extract any useful information.

If you provide VSP Form with an e-mail address for you and/or the customer, it also sends confirmation e-mails in the event of a successful order. If the order fails, you are mailed with detail and reasons but the customer is not.

PROTX provide Integration Kits, which are simple worked examples in various different scripting languages that perform all the tasks described above. You simply customise these to work with your particular environment. So whether you are running .NET, ASP, PHP, Coldfusion or PERL, and whether your servers are Linux Apache, Win32 IIS or Domino, we’ve already done half of the work for you.

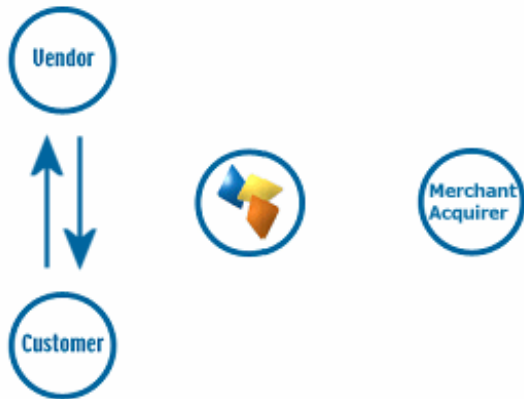
The following sections explain the integration process in more detail. The complete VSP Form Payment protocol is attached in the appendix, providing a detailed breakdown of the contents of the encrypted fields sent between your servers and ours during a payment.



The VSP Form Payment Process in Detail

This section details the messages exchanged between your Web servers and the VSP Form 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 Form system puts no requirement on you to collect any specific set of information.

It is generally a good idea to identify the customer by name, e-mail address, delivery and billing address and telephone number. You should store these details in your session alongside details of the customer's basket contents or other ordered goods. **YOU DO NOT NEED TO COLLECT CREDIT OR DEBIT CARD DETAILS.** All your site needs to do is calculate the total cost of the order in whatever currency your site operates and present the user with a confirmation page, summarising their order, containing the transaction detail in an encrypted hidden field (see below).

Step 2: Your server builds a Confirmation Page.

Your server-side script will build an order confirmation page, displaying the full details of the purchase to the customer, including their billing and delivery addresses, basket contents, total order value and contact details.

This script will also place a form on that page with the action set to the Protix VSP Form registration page. That form will also contain four hidden fields:

- **VPSPProtocol** - which lets our system know you are using protocol 2.22.
- **TxType** - which tells you are making a PAYMENT or other transaction type, see later.
- **Vendor** - which is your unique company identifier assigned to you by Protix.
- **Crypt** – A field containing encrypted and encoded details of the transaction to prevent the customer from being able to tamper with the contents before they are submitted to us.

The contents of the crypt field are built by your script and include, amongst other things:

- A unique reference to this transaction that you generate (the VendorTxCode).
- Total transaction value and currency.
- The URLs of the order Success and Failure pages.

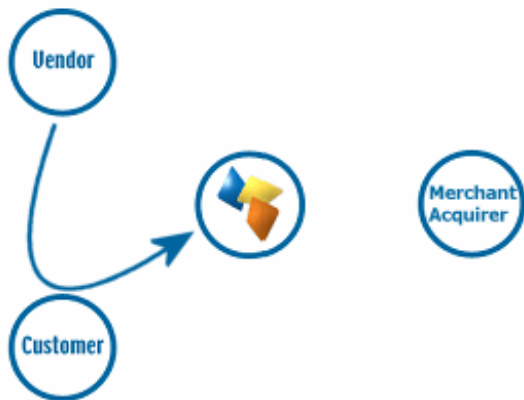
VSP Form Protocol and Integration Guidelines



- Customer e-mail address for confirmation e-mails.
- Your e-mail address for notification e-mails.
- Billing and Delivery Addresses and Post Code.
- Basket Contents and a Description of Goods.

See Appendix A for the full protocol which lists all the fields you can send if you wish, and those which are compulsory for all transactions.

The integration kits we provide contain scripts in a variety of languages that illustrate how you build this encrypted field so don't worry if this all sounds a bit involved. Please contact info@protx.com if you would like us to send you a specific kit.



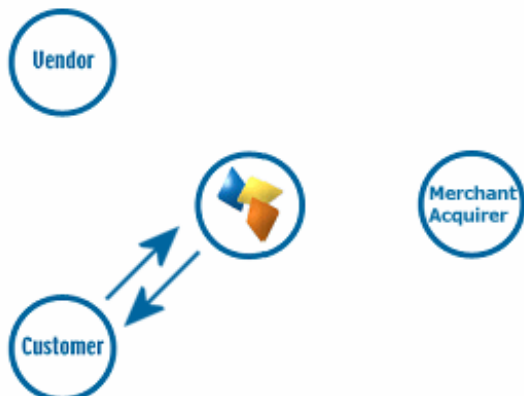
When the customer clicks the "Pay Now" button on the form, the hidden field is POSTed to VSP Form and the customer's browser is redirected there.

VSP Form begins by validating the Crypt field 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 and validation error is displayed on screen. This normally only happens in the development stage so your customers are unlikely to encounter this page.

If all fields are present and correct, the information in those fields is then validated. The Vendor name is checked against our database and 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 and the Basket contents are validated to ensure they have been sent in a format VSP Form understands.

If everything in the original POST checks out, the transaction is registered with VSP Form system and 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 sent back to you at the transaction completion stage.

Step 3: Customer enters card details on VSP Form.



The customer is presented with a page requesting their credit/debit card details. This page will contain your company logo and the description of goods passed in Step 2 above. You can elect to customise these pages further by producing your own custom templates (please contact support@protx.com if you require more information about custom templates)

Once the customer has entered their

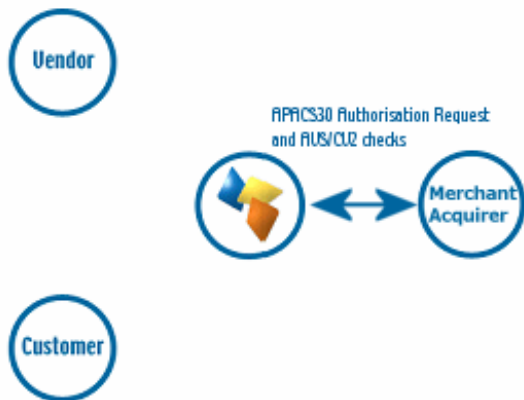


details, the VSP Form system verifies their details, prior to communicating with the bank, to ensure the card number is valid, the card type matches the card number, the expiry date is not in the past and, where appropriate, the issue number and start date are in the correct format.

If valid card details have been entered, the customer is presented with a confirmation screen where they have one last chance to change their mind and cancel the transaction. If the customer decides to cancel, you will be sent a cancellation message to your Failure URL (see later).

If the customer wishes to continue, the VSP Form initiates the process of obtaining an authorisation code from the merchant acquirer.

Step 4: VSP Form requests card authorisation.



The VSP Form sends an internal, secure message from our front-end processing systems to the back-end authorisation boxes, over our own private network.

The VSP authorisation services then format an APACS30 message and send the request to your merchant acquirer over the X25 banking network.

The request is normally answered within a second or so with either an authorisation code, or a failure message.

Whilst communicating with the merchant acquirer, the customer is shown a page containing the text, "Authorising please wait..."

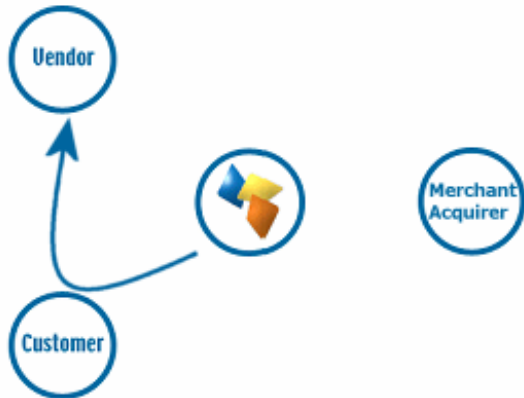
The VSP Form system handles all authorisation failures in the same way, replying to your site with a NOTAUTHED message and a blank authorisation code.

If the acquirer does return an Authorisation code, VSP Form prepares an OK to send back to you (next step)

If fraud checks are being performed, the results are compared to any rule bases you have set up (see the Fraud Screening companion documentation for more information). If the bank has authorised the transaction but the card has failed the fraud screening rules you have established, PROTX immediately reverse the authorisation with the bank, clearing the charge on the card, and prepare a REJECTED response for your web site.



Step 5: VSP Form Redirects the Customer to your site.



Depending on the result of the authorisation with the bank, your customer is either returned to your SuccessURL (the successful order completion page you supplied in step 2), or your FailureURL for all other transactions.

Appended to the SuccessURL or FailureURL is an encrypted field, again called Crypt, which contains the status of the transaction, the reference codes for those transactions and the results of fraud checking. This field is decoded in

the same manner that your original script was encoded, using the same password (which is known only to you). The contents of the Crypt field are detailed in Appendix A2.

The Status field holds either **"OK"**, if the transaction was authorised at step 4, **"NOTAUTHED"** if the authorisation was failed by the bank, **"ABORT"** if the user decided to cancel the transaction whilst on the PROTX site, **"REJECTED"** if authorisation occurred but your fraud screening rules were not met, or **"ERROR"** if something serious has occurred at PROTX, for example database failure, or all X25 links down.

The StatusDetail field contains a human readable description of the error message.

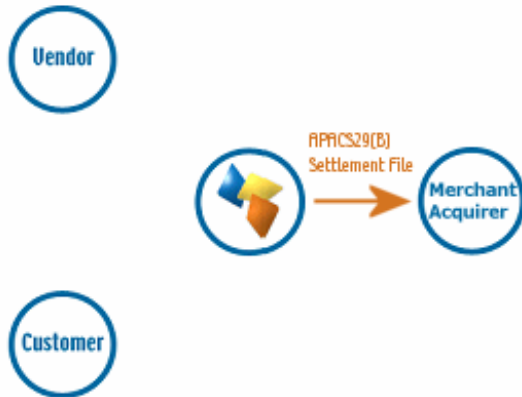
You may wish to display some of the information contained in the crypt field to your customer, especially the reason for failure (if authorisation could not be taken). You are not required to store any of the information sent to you in a database, but if you have access to one, you may wish to do so.

You will receive an e-mail (if you supplied a VendorEMail address) with all these details in, plus details of the order and the customer who placed it. Protx cannot guarantee that e-mail will always arrive, however, since we have no control over what happens to it when it leaves our servers. You should not rely solely on e-mail confirmation, but regularly check your VSP Admin pages for new orders (see later).

The real time processing of the transaction by Protx is now complete.



Step 6: VSP sends daily Batch File to confirm payments.



Once per day, at 2:00am, the VSP Form system takes all authorised transactions for each acquirer and creates an APACS29b format batch file.

Transactions for ALL vendors 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.

These files 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 30-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 service 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, but in many cases PROTX have to wait for the acquirers to send paper confirmation through the post to check that the file was accepted and no transactions were rejected. 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 Form

Linking your Web site to VSP Form involves creating one script (or modifying the example provided in the integration kits), and two completion pages, one for successful transactions, the other for failures.

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 Form.

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/VSPFormGateway.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. 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 runs 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 Form at:

<https://ukvpstest.protx.com/vps2Form/submit.asp>

Stage 3

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, we set up your account on the live server (after a request from you to golive@protx.com). 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 Form at:

<https://ukvps.protx.com/vps2Form/submit.asp>



Stage 1: Integrating with the VSP Simulator

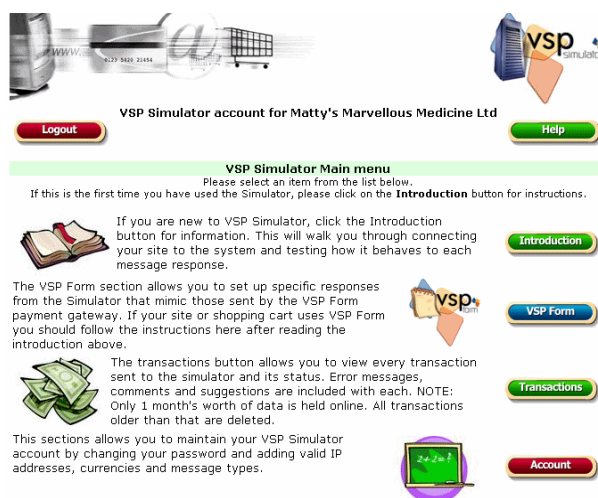
The VSP Simulator is an expert system that emulates the VSP Form system and allows you to develop your site to correctly send and process the messages exchanged between your site and ours. VSP Simulator will provide more detailed feedback of any errors or issues than the real VSP Form, allowing you to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

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://www.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) and 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:

VSP Simulator account for Tony's Toupees

Administrative Functions - Account Administration

This screen allows you to modify your VSP simulator account settings by adding IP Addresses, currencies accepted and payment options. You can also change your password from here. **IMPORTANT NOTE:** None of these changes will be migrated across to the Protx test or live servers unless you update your online application for with the new details!

Account Settings

Company Display Name:	Tony's Toupees
Full Home Page URL:	http://www.protx.com
Your contact e-mail address:	Tony.Welch@protx.com
Simulate VSP Form:	<input type="checkbox"/>
Simulate VSP Server:	<input checked="" type="checkbox"/>
Simulate VSP Direct:	<input type="checkbox"/>
Enable PREAUTH & REPEAT transactions:	<input type="checkbox"/>
Enable DEFERRED & RELEASE transactions:	<input type="checkbox"/>
Operating System:	(none selected)
Scripting Language:	ASP
Shopping Cart Used:	(none selected)

Valid IP Addresses for this Account

These IP Addresses list ONLY those servers at your site which DIRECTLY connect to either VSP Server or VSP Direct. VSP Form users do not need to list the IP addresses of the machines they use.

PROTX Internal IP Address for VSP Admin (cannot be removed)

☐ 213.052.206.220 (255.255.255.255)

Click the Delete button to remove any selected IP addresses

Add New IP: **Subnet Mask:** **Add**

Valid Currencies for this Account

Only transaction registrations for amount in the following Currencies will be accepted by the VSP Simulator. You should ensure you have e-commerce merchant numbers for all currencies your site wishes to support.

☐ GBP

Click the Delete button to remove any selected currencies

Add New Currency: AUD - Australian Dollar **Add**

Change Password

Current Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirm New Password:	<input type="password"/>

Set Password

Click the Back button to go back to the main menu. **Back**

You should ensure that:

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

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

There is nothing more for you to set up in VSP Simulator. The VSP Form component takes care of everything itself, so for now, click Back, then log out of VSP Simulator.

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 info@protx.com

This script provides a worked example of how to construct the Crypt field that VSP Form need to initiate the payment process (see Appendix A section A1 in the attached protocol).



VSP Simulator

Account for



Help

VSP Form Payment Gateway

This page emulates the VSP Form submission pages. The information sent to this page via the customer's browser in the encrypted fields are decoded here and broken down for you to check. Any errors will be reported here, along with recommendations. If there are no errors, you will be able to **Proceed** to the payment simulation pages.

Fields in your VSP Form Submission POST

The following fields were included in the FORM sent to the VSP Form submission page.

VSPProtocol: 2.22	
TextType: PAYMENT	
Vendor: matty	
Crypt: Present - See decoded section below	

VSP Form decoded the Crypt field as follows.

VendorTxCode=matty-200503171043-165173&Amount=39.60&Currency=GBP&Description=Quality nosh and berries from ShuklasSuccessURL=http://TEAPOT/shuklas/VSPFormCompleted.asp&FailedURL=http://TEAPOT/shuklas/VSPFormFailed.asp&CustomerName=Mat Peck&CustomerEmail=Mat.Peck@protx.com&VendorMail=Mat.Peck@protx.com&BillingAddress=22 Soho Square London&BillingPostCode=W1D 4NS&DeliveryAddress=22b Baker Street London&DeliveryPostCode=W8T 5ON&ContactNumber=0207-292-3900&ContactFax=0207-292-3900&AVSCV2=0&ApplyAVSCV2=0&Apply3DSecure=0&Basket=1-Ben and Jerry's Chocolate Fudge Brownie:12f2.81f0.49f3.30f39.60&MailMessage=Thank you for shopping at Shuklas. Please come again, only next time spend more money!

VSP Form extracted the following fields from the Crypt field.

VendorTxCode: matty-288503171043-165173	The VendorTxCode is valid.
Amount: 39.60	The Amount is valid.
Currency: GBP	The Currency is valid.
Description: Quality nosh and berries from Shuklas	The Description is valid.
SuccessURL: http://TEAPOT/shuklas/VSPFormCompleted.asp	The SuccessURL is valid.
FailureURL: http://TEAPOT/shuklas/VSPFormFailed.asp	The FailureURL is valid.
CustomerName: Mat Peck	The CustomerName is valid.
CustomerMail: Mat.Peck@protx.com	The CustomerMail is valid.
VendorEmail: Mat.Peck@protx.com	The VendorEmail is valid.
EmailMessage: Thank you for shopping at Shuklas. Please come again, only next time spend more money!	
BillingAddress: 22 Soho Square London	The BillingAddress is valid.
BillingPostCode: W1D 4NS	The BillingPostCode is valid.
DeliveryAddress: 22b Baker Street London	The DeliveryAddress is valid.
DeliveryPostCode: W8T 5ON	The DeliveryPostCode is valid.
ContactNumber: 0207-292-3900	The Contact Number is valid.
ContactFax: 0207-292-3900	The ContactFax is valid.

Basket Contents (1 line(s) of detail)

Item	Quantity	Unit Item Value	Item Tax	Item Total	Line Total
Ben and Jerry's Chocolate Fudge Brownie	12	£2.81	£0.49	£3.30	£39.60

The Basket is valid.

AllowofftAid: 0 The AllowofftAid flag is valid.

ApplyAVSCV2: 0 The ApplyAVSCV2 flag is valid.

Apply3DSecure: 0 The Apply3DSecure flag is valid.

Proceed

The top section of the screen validates the hidden fields, ensuring your protocol version is correct, your transaction type is valid and your vendor name is known. If anything is incorrect, you will be informed of the error.

The Proceed button only appears if there are no red errors.

VSP Form Protocol and Integration Guidelines



This page is for information only and shows you what the customer would be seeing at this stage in the real VSP Form system. It explains the type of messages our system might generate and under what circumstances.

VSP Form Payment Page

At this point during the process, your customer will be seeing the payment page as shown below.

Your company logo will appear in the top left corner, where the Shukla's logo is displayed. The Test Server logos and associated text only appear on the Test Server to ensure you never inadvertently direct users to the test system whilst intending to take Live transactions.

Your description of goods from the **Description** field along with your company name and the **Amount** and **Currency** fields are then displayed.

The customer will enter their payment card details in the subsequent boxes and confirm their **BillingAddress** and **BillingPostCode** as optionally supplied in the registration POST.

They will then press **Proceed** and confirm at a subsequent page that they wish to continue.

VSP Form then requests an authorisation from the bank and processes the response. If the card is accepted, VSP Form sends an **OK** message back to your server, along with the authorisation codes.

If the bank declines the card, the customer is given two additional attempts to make a valid payment before a **NOTAUTHED** message is sent back to your site.

Should the user click **Cancel**, an **ABORT** message is sent.

REJECTED is sent back if the bank did authorise the transaction but rules that you have created governing AVS/CV2 or 3D-Secure results have caused the VSP systems to automatically reverse and reject the payment.

ERROR is sent if something is wrong with the payment systems or authorisation process.

Proceed



The completion page allows you to select which type of response you wish to send back to your server.

VSP Form Payment Page - Authorisation Options

The responses outlined in the protocol and previous page can be simulated using the buttons below. These messages will be compiled, encrypted, encoded and passed to the **SuccessURL** (for **OK** messages) or the **FailureURL** (for all other message types) in a querystring field called **Crypt** (in the same manner as the real VSP Form system). The URLs you provided were:

SuccessURL : <http://TEAPOT/shuklas/VSPFormCompleted.asp>

FailureURL : <http://TEAPOT/shuklas/VSPFormFailed.asp>

Results of AVS, CV2 and 3D-Secure Checks

Use the Radio buttons below to select the AVS, CV2 and 3D-Secure results if you wish. By changing these values you can write code in your completion pages that make decisions based on the results of the security checks. NOTE: The Gift Aid check box enables you to set the value of the GiftAid field (useful for UK registered charities).

Address Check Result:	<input type="radio"/> NOTPROVIDED <input type="radio"/> NOTCHECKED <input type="radio"/> NOTMATCHED <input checked="" type="radio"/> MATCHED
Post Code Check Result:	<input type="radio"/> NOTPROVIDED <input type="radio"/> NOTCHECKED <input type="radio"/> NOTMATCHED <input checked="" type="radio"/> MATCHED
CV2 Check Result:	<input type="radio"/> NOTPROVIDED <input type="radio"/> NOTCHECKED <input type="radio"/> NOTMATCHED <input checked="" type="radio"/> MATCHED
3D-Secure Result:	<input type="radio"/> NOTAVAILABLE <input type="radio"/> NOTAUTHED <input type="radio"/> INCOMPLETE <input type="radio"/> ERROR <input checked="" type="radio"/> OK
Gift Aid Selected?:	<input type="checkbox"/> (check to simulate a customer electing to donate tax on this payment)

VSP Form Status to send to the Completion URLs

Clicking one of the buttons below will format a message of that type, compile a **Crypt** field and redirect the browser to the appropriate completion page, passing the data. You can test the function of your completion pages by sending each message type and adjusting your messages to your customers appropriately.

The OK response is sent when a transaction is successfully authorised. The customer will be redirected to the SuccessURL page which should store the TxAuthNo field against the transaction details in your database, along with any other details you wish to store, before presenting the customer with successful completion details.	<input type="button" value="OK"/>
The NOTAUTHED response is sent if the bank has declined the transaction three times. The user has had multiple chances to enter a valid card but none have been authorised. The customer is redirected to the FailureURL when this occurs.	<input type="button" value="NOTAUTHED"/>
The MALFORMED message is only sent if the Transaction Registration POST is poorly formatted. This should not occur in a live environment (in fact, because you have reached this stage your code is already sending correct messages). You should code your FailureURL to be able to handle messages of this type, however.	<input type="button" value="MALFORMED"/>
The INVALID message is only sent if the Transaction Registration POST contains illegal data. Like the MALFORMED message, this should not occur in a live environment, but you should also code your FailureURL to be able to handle messages of this type.	<input type="button" value="INVALID"/>
The ABORT message is sent when the user clicks the Cancel button on the payment page, or if they close their browser, it is sent after 15 minutes of inactivity. You may wish to code your FailureURL to produce a page asking the user if they need assistance with their order when such messages are sent.	<input type="button" value="ABORT"/>
The REJECTED message is sent if the banks authorised the payment but the AVS, CV2 or 3D-Secure rulebases you have set up caused the VSP System to automatically cancel that authorisation because those security criteria were not met. Your FailureURL may wish to display a message to this effect, or you may simply wish to inform the customer that their payment could not be accepted.	<input type="button" value="REJECTED"/>
The ERROR message is only sent if something has gone wrong at PROTX. You'll receive this message very rarely (occasionally during schedule dmaintenance) but your FailureURL code should be written to handle it.	<input type="button" value="ERROR"/>

An OK message, indicating an authorised transaction, would redirect you back to your success page, as passed in the SuccessURL field.

All other message types are set to the FailureURL, along with the reason for failure in the StatusDetail field.

You can also chose the exact fraud screening results you wish to send back, to enable you to develop code that responds to these values if you wish. By default the example in the kits simply display them.



3: 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.

VSP Simulator account for Tony's Toupees

Logout Help

Transaction List

This screen provides you a list of all transactions of each type you have sent to the Simulator over the last month. You have the option to sort those transactions by VendorTXCode or Date. Click on a VendorTXCode, or the system icon, to bring up the full details of the selected transaction.

VSP Systems used to process the transaction

☒ VSP Server ☒ VSP Form ☒ VSP Direct

Sort Order: Date/Time Received ☐ Transaction Code ☐
Descending ☐ Ascending ☐

Proceed

VSP	VendorTXCode	Received	Amount	VSP 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.		
	Test791668117	23/02/05 10:05:30	40.00 (GBP)	0	Transaction registered and user successfully redirected to the payment pages.		
GBP Total:			80.00 (GBP)				

Click the Back button to go back to the main menu.

Back

VSP Simulator Transaction Details

The tables below show all the information held by VSP Simulator about the selected transaction. Once you've examined the information, click Back to go back to the transaction list.

PAYMENT transaction

Transaction Information

Vendor TX Code: Test713512599
 VPSiteID: (CF4DEADD-6811-4016-878D-91CEAF81E489)
 Security Key: 3XU33Q3LE1
 Status: Transaction registered and user successfully redirected to the payment pages.
 Description: SomeShopFromProbz
 Amount: 40.00 (GBP) System Used: VSP Server
 Authorized: Yes VSP Auth Code: 0
 Started: 23 February 2005 at 10:09:36
 Refunded: No Repeated: No
 User: VSP Simulator Gift Add: No
 Notification URL: http://192.168.0.143/ASPServer/VSPHandlePROTXResponse.asp

Customer Details

Customer Name:
 Client ID: 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

Click the Back button to go back to the main menu.

Back

You can also see from this screen which transactions have been subsequently refunded or used as the basis for repeat payments (see 4 below).

Once your site can initiate transactions AND handle the callbacks, then you've completed your basic VSP Form integration and can move on to testing your site against the real VSP Form, firstly on the Test Server.



4: 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, 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 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. If you take longer than that to ship the goods, you should look at the PREAUTH and REPEAT method described below, because cards are only shadowed for a limited period of time (normally 3-5 days at most depending on who issued the card) and if the shadow disappears 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.

PREAUTH and REPEAT transactions.

IMPORTANT INFORMATION REGARDING PREAUTHS

As of 1st November 2006 we can no longer provide the PreAuth payment type as an option to new ProtX vendors. The PreAuth payment type will still work for existing vendors who already have the payment type enabled, but only until 31st May 2007.

As of 1st June 2007 the PreAuth payment type will no longer be a service that ProtX provide. An alternative to the PreAuth payment type will be available, full details of this will be provided to all ProtX vendors in January 2007.

Like DEFERRED, PREAUTH transactions are registered in exactly the same way as PAYMENTS but with the TxType set to PREAUTH instead.



A PREAUTH requests an authorisation against the card, but if one is obtained it is instantly reversed, cancelling the shadow so the customer is not inconvenienced. No funds are transferred to your account, nor can they ever be. It does, however, confirm that the card is valid and has available funds at the time of the PREAUTH. It also provides fraud screening results like any normal payment.

At a later date, for example when you are ready to ship goods, you send a REPEAT payment request using the Repeat button in the VSP Admin system, to charge that card with the full value of the transaction without the need for you to hold the customer's card details anywhere on your servers (removing the need for you to worry about securing such sensitive data).

PREAUTH/REPEAT is useful when there is a long delay between order and fulfilment (since DEFERRED shadows only last so long), or if you are uncertain of the exact value of the transaction at the time of order (common with weight sensitive products), or if you wish to take recurring payments against a card for membership or monthly subscriptions because it removes the need for you to store card details.

The REPEAT payment is authorised and settled on the same day, like a regular PAYMENT, so there is no chance of funds not being available if the REPEAT is authorised. There IS, however, the possibility that between the PREAUTH being taken and the REPEAT being requested, the customer will have maxed out their card and no funds will be available for the REPEAT payment. In such circumstances you should not complete the order and should contact the customer for alternative methods of payment.

REFUNDS and VOIDS

Once a PAYMENT or REPEAT has been authorised, or an authorised 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 through the VSP Admin interface to prevent the transaction ever being settled. 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 use the VSP Admin screens to REFUND the transaction instead.

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.



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://www.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 Form 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/vps2Form/submit.asp>

When your site redirects the customer you will find yourself on the real Protix payment pages rather than the Simulator.

Here, during testing, you can use any of the test card numbers on the following page (provided your account can handle cards of those types) or you can use your own cards if you wish (since there is no chance of them actually being authorised, and the security on the test server is as high as it is on live, so there is no chance of them being compromised). Any cardholder name and start/expiry dates will be accepted for these cards so long as the dates are valid and the card current.



Card Type	Card Number	Issue Number
VISA	4929 0000 0000 6	None
MasterCard	5404 0000 0000 0001	None
Delta	4462 0000 0000 0003	None
Solo	6334 9000 0000 0005	1
Switch/UK Maestro	5641 8200 0000 0005	01
AMEX	3742 0000 0000 004	None
Diner's Club	3600 0000 0000 08	None

The process will then continue as per the Live Servers only the authorisation stage is simulated. You will always receive an OK message and an Authorisation Code from the test server unless you send a specific amount and use a specific card and expiry date (the support team will give you details when your account is set up).

Once you've checked you can process an end-to-end transaction then you are almost ready to go live. Before doing so, however, you should log in to the 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>



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.

VSP Form Protocol and Integration Guidelines



- In the **Password** box, enter the VSP Admin password as supplied to you by Protix when your test account was set up.
- Click **Login**.

securing future e-commerce

Current Vendor: **Protix Ltd**
Current User: **protix**

Logout | Help | How To... | Updates | Administration

Administrative Functions - User Account Management
This screen allows you to Add, View and Maintain users with access to your Protix VSP account. Only the main Administrative account cannot be modified from here (you will need to contact Protix if that account has become locked out or you require a password change).

User Name	Access Level	Logged In?	Locked Out?	Actions
Admin Account (protix)	IMPORTANT! 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 Protix if you need assistance.

Or to create a new User Account, click here: **Add**

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 | How To... | 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.
Transaction List: ☒ 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.

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 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 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 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/vps2Form/submit.asp>

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.

You should then log into the Live Server VSP Admin screens at <https://ukvps.protix.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 Form

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 Protix invoice, or have a general question about online payments or fraud, e-mail info@protix.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@protix.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 e-mail feedback@protix.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, e-mail beta@protix.com and let us know your VSP Vendor Name so we can include you in the scheme.
- You can call us as well on 0207-292-3900, 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.protix.com/services/monitorvsp.asp>

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



Appendix A - The VSP Form Protocol v2.22

This section details the VSP Form Protocol transaction registration POST, and the contents of the Crypt fields passed back and forth between your web site and ours.

A1: Transaction registration

The final confirmation page on your web site should contain an HTML FORM with the Action set to the Protix VSP Form submission URL and the following 4 hidden fields as part of that Form.

Form Fields

Name	Format	Values	Comments
VPSProtocol	Alphanumeric. Fixed 4 characters.	"2.22" in this release	Default or incorrect value is taken to be 2.1
TxType	Alphanumeric Max 15 characters.	"PAYMENT", "DEFERRED" or "PREAUTH"	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 Protix when your account was created.
Crypt	Alphanumeric Max 16k characters	All other transaction information, encrypted then encoded. See below.	Your site builds the Crypt field in real time for each order. The contents of the field are described below.

The Crypt Field

The Crypt field should contain all the other transaction information (see the next section) in plain text as Name=Value fields separated by '&' characters. This string should then be encrypted using a Simple XOR algorithm and the pre-registered password (in the case of the test vendor, the password is also "testvendor") and subsequently Base64 encoded to allow safe transport in an HTML form.

The functions to perform these steps (SimpleXor and Base64Encode) are included in the kits and can be used in your own script pages.

VSP Form Protocol and Integration Guidelines



Crypt Field Contents (continued overleaf)

Name	Format	Values	Comments
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 on the VSP Form payment page as the customer enters their card details.
SuccessURL	Alphanumeric Max 2000 characters	Full qualified URL (including http:// or https:// header).	The URL of the page/script to which the user is redirected if the transaction is successfully authorised. You may attach parameters if you wish, but the VSP will also send an encrypted field containing important information appended to this URL (see below).
FailureURL	Alphanumeric Max 2000 characters	Full qualified URL (including http:// or https:// header).	The URL of the page/script to which the user is redirected if the transaction is not authorised, aborted or an error occurs. You may attach parameters if you wish, but the VSP will also send an encrypted field containing important information appended to this URL (see below).
Optional: CustomerName	Alphanumeric Max 100 characters	The customer's name.	If provided the customer's name will be included in the confirmation e-mails and stored in the VSP Admin area.
Optional: CustomerEMail	Alphanumeric Max 255 characters	The customer's e-mail address. NOTE: If you wish to use multiple email addresses, you should add them using the : (colon) character as a separator. e.g. myemail@myemail.com : anotheremail@anotheremail.com	If provided, the customer will be e-mailed on completion of a successful transaction (but not an unsuccessful one).
Optional: VendorEMail	Alphanumeric Max 255 characters	An e-mail address on which you can be contacted when a transaction completes. NOTE: If you wish to use multiple email addresses, you should add them using the : (colon) character as a separator. e.g. myemail@myemail.com : anotheremail@anotheremail.com	If provided, an e-mail will be sent to this address when each transaction completes (successfully or otherwise)
Optional: eMailMessage	Alphanumeric Max 7500 characters	A message to the customer which is inserted into the successful transaction e-mails only.	If provided this message is included toward the top of the customer confirmation e-mails.

VSP Form Protocol and Integration Guidelines



Optional: BillingAddress	Alphanumeric Max 200 characters	Free format field for the customer's Billing Address without the Post/Zip code	If provided this information will populate the Billing Address edit box on the card input screens.
Optional: BillingPostCode	Alphanumeric Max 10 characters	The Post code or Zip code of the customer's billing address	If provided this information will populate the Billing Post Code edit box on the card input screens.
Optional: DeliveryAddress	Alphanumeric Max 200 characters	Free format field for the customer's Delivery Address without the Post/Zip code	This information is not used in AVS checks but is held on the reporting systems for your records.
Optional: DeliveryPostCode	Alphanumeric Max 10 characters	The Post code or Zip code of the customer's delivery address	This information is not used in AVS checks but is held on the reporting systems for your records.
** NEW ** Optional: ContactNumber	Alphanumeric Max 20 characters	The telephone number on which to contact the customer.	The information is not used in customer validation at present and is available for reporting purposes only.
** NEW ** Optional: 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.
Optional: Basket	Alphanumeric Max 7500 characters	See the next page for the Format of the Basket field	This field can use to supply details of the customer's order. Future versions of the system will use this field to supply Line Item detail for purchase cards.
** NEW ** Optional: AllowGiftAid	Flag	0 = No Gift Aid Box displayed (default) 1 = Display Gift Aid Box on payment screen.	This flag allows the gift aid acceptance box to appear for this transaction on the payment page. This only appears if your vendor account is Gift Aid enabled.
** NEW ** Optional: ApplyAVSCV2	Flag	0 = If AVS/CV2 enabled then check them. If rules apply, use rules. (default) 1 = Force AVS/CV2 checks even if not enabled for the account. If rules apply, use rules. 2 = Force NO AVS/CV2 checks even if enabled on account. 3 = Force AVS/CV2 checks even if not enabled for the account but DON'T apply any rules.	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.
** NEW ** Optional: Apply3DSecure	Flag	0 = If 3D-Secure checks are possible and rules allow, perform the checks and apply the authorisation rules. (default) 1 = Force 3D-Secure checks for this transaction if possible and apply rules for authorisation. 2 = Do not perform 3D-Secure checks for this transaction and always authorise. 3 = Force 3D-Secure checks for this transaction if possible but ALWAYS obtain an auth code, irrespective of rule base.	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.



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 of item 1:
Cost of Item 1 inc tax:
Total cost of item 1 (Quantity x cost inc tax):
Item 2 Description:
Quantity of item 2:
....
Cost of Item n inc 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: Transaction Completion

In FORM based transactions, ProtX cannot guarantee to return the customer to your web site. If the customer closes their browser mid-way through a transaction, or if something goes wrong at any redirect stages, it will be up to you to check the status of the transactions on the VSP Admin reporting screens.

In normal circumstances, however, where the customer does not close their browser and there are no redirection problems, VSP Form will return them to your site, either to the SuccessURL (in the event the authorisation was successful), or the FailureURL (in all other circumstances).

The VSP will append to the SuccessURL or FailureURL a field called CRYPT, in the manner:

[ResponseURL]?crypt=[encrypted_information]

or if the URL already has your own fields attached, it will be appended thus:

[ResponseURL]?vendor1=test&vendor2=test2&crypt=[encrypted_information]

The SuccessURL and FailureURL field should point to scripts on your server that extract the information in the crypt field and use it to update your database (if you have one) and/or format an appropriate response page for the customer. This is not compulsory, however, and you may choose to simply direct customers to a static HTML page that ignores the contents of the crypt field. In such cases, you will need to manually check the VSP Admin report pages to determine if a transaction succeeded or failed. In fact, we recommend you always check the VSP Admin pages before sending any good just to confirm the status of each transaction.

The Crypt field contains the plain text shown overleaf as Name=Value fields separated by '&' characters, subsequently encrypted using the simple XOR routine and your pre-registered password, then Base64 encoded. Exactly the same process your scripts performed at the transaction registration stage. To read the contents, you must Base64 decode the field, then XOR it with your password, then split the contents out into manageable fields. Routines to perform this (Base64Decode, SimpleXOR and GetToken) are included in the kits and can be used in your own script pages.



Response Crypt Field Contents (continued overleaf)

Name	Format	Values	Comments
Status	Alphanumeric Max 20 characters	<p>"OK" – Transaction completed successfully with authorisation.</p> <p>"NOTAUTHED" – The VSP system could not authorise the transaction because the details provided by the Customer were incorrect, or not authenticated by the acquiring bank.</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>"ABORT" – The Transaction could not be completed because the user clicked the CANCEL button prior, or went inactive for 15 minutes or longer.</p> <p>"ERROR" – A code-related error occurred which meant the Transaction could not be completed successfully.</p> <p>** NEW **</p> <p>"REJECTED" – The VSP System rejected the transaction because of the rules you have set on your account.</p>	<p>In the case of NOTAUTHED, the Transaction has completed through the VSP System, but it has not been authorised by the bank.</p> <p>A status of REJECTED means the bank may have authorised the transaction but your own rule bases for AVS/CV2 or 3D-Secure caused the transaction to be rejected.</p> <p>In the cases of ABORT, MALFORMED, INVALID and ERROR (see below) the Transaction has not completed through the VSP and can be retried.</p> <p>Please notify PROTX if a Status report of ERROR is seen, together with your VendorTxCode and the StatusDetail text.</p>
StatusDetail	Alphanumeric Max 255 characters	Human-readable text providing extra detail for the Status message	You should always check this value if the Status is not OK .
VendorTxCode	Alphanumeric Max 40 characters	Your unique Vendor Transaction Code	Same as sent by your servers in Step A1.
VPSTxId	Alphanumeric 38 characters	The ProtX ID to uniquely identify the Transaction on our system.	Only present if Status is OK , NOTAUTHED , ABORT or REJECTED .
TxAuthNo	Long Integer	ProtX unique Authorisation Code for a successfully authorised transaction.	Not present if Transaction was not successfully authorised (Status not OK).
Amount	Numeric	The total value of the transaction.	Should match that sent in A1. Included to allow non-database driven users to react to the total order value.
AVSCV2	Alphanumeric Max 50 characters	Response from AVS and CV2 checks. Will be one of the following: "ALL MATCH" , "SECURITY CODE MATCH ONLY" , "ADDRESS MATCH ONLY" , "NO DATA MATCHES" or "DATA NOT CHECKED" .	<p>Provided for Vendor info. Rules set up at the VSP server will accept or reject the transaction based on these values.</p> <p>More detailed results are split out in the next three fields.</p>

VSP Form Protocol and Integration Guidelines



** NEW ** AddressResult	Alphanumeric Max 20 characters	"NOTPROVIDED", "NOTCHECKED", "MATCHED", "NOTMATCHED"	The specific result of the checks on the cardholder's address numeric from the AVS/CV2 checks.
** NEW ** PostCodeResult	Alphanumeric Max 20 characters	"NOTPROVIDED", "NOTCHECKED", "MATCHED", "NOTMATCHED"	The specific result of the checks on the cardholder's Post Code from the AVS/CV2 checks.
** NEW ** CV2Result	Alphanumeric Max 20 characters	"NOTPROVIDED", "NOTCHECKED", "MATCHED", "NOTMATCHED"	The specific result of the checks on the cardholder's CV2 code from the AVS/CV2 checks.
** NEW ** GiftAid	Flag	0 = The Gift Aid box was not checked this transaction. 1 = The user checked the Gift Aid box on the payment page	This field is always present even if GiftAid is not active on your account.
** NEW ** 3DSecureStatus	Alphanumeric Max 50 characters	"OK" - 3D Secure checks carried out and user authenticated correctly. "NOTAVAILABLE" – The card used was either not part of the 3D Secure Scheme, or the authorisation was not possible. "NOTAUTHED" – 3D-Secure authentication checked, but the user failed the authentication. "INCOMPLETE" – 3D-Secure authentication was unable to complete. No authentication occurred. "ERROR" - Authentication could not be attempted due to data errors or service unavailability in one of the parties involved in the check.	This field details the results of the 3D-Secure checks (where appropriate)
** NEW ** CAVV	Alphanumeric Max 32 characters	The encoded result code from the 3D-Secure checks.	Only present if the 3DSecureStatus field is "OK"