Virtual
card services

Divert to ccForm
Interfacing Specification

Last modified November 2009

Contact Details:
Skype: vcs.support
MSN: support@vcs.co.za
E-mail: support@vcs.co.za
Phone Support: 010 590 1919
Phone SwitchB: 087 940 1917

Table of Contents

1. INTRODUCTION

The purpose of this document is to provide the web developer with a sample layout of how to interface with the generic VCS secure credit card payment page.

The merchant's website does not have to be secure, VCS provides the security.

To interface with this service requires the web developer to divert the browser to VCS.

2. AUTHORISATION REQUEST

The merchant's check out page has to contain the following form with a submit button to "POST" the cardholder's browser to the VCS website.

2.1 Example HTML code

```
<form method="POST" action="https://www.vcs.co.za/vvonline/ccform.asp">
        <input type="hidden" name="p1" value="a">
        <input type="hidden" name="p2" value="b">
        <input type="hidden" name="p3" value="c">
        <input type="hidden" name="p4" value="d">
        <input type="hidden" name="p5" value="e">
        <input type="hidden" name="p6" value="f">
        <input type="hidden" name="p7" value="g">
        <input type="hidden" name="p8" value="h">
        <input type="hidden" name="p9" value="i">
        <input type="hidden" name="p10" value="j">
        <input type="hidden" name="p11" value="k">
        <input type="hidden" name="p12" value="l">
        <input type="hidden" name="p13" value="m">
        <input type="hidden" name="Budget" value="n">
        <input type="hidden" name="NextOccurDate" value="o">
        <input type="hidden" name="CardholderEmail" value="p">
        <input type="hidden" name="Hash" value="q">
        <input type="hidden" name="m_1" value="z">
        <input type="hidden" name="m_2" value="z">
        <input type="hidden" name="m_3" value="z">
        <input type="hidden" name="m_4" value="z">
        <input type="hidden" name="m_5" value="z">
        <input type="hidden" name="m_6" value="z">
        <input type="hidden" name="m_7" value="z">
        <input type="hidden" name="m_8" value="z">
        <input type="hidden" name="m_9" value="z">
        <input type="hidden" name="m_10" value="z">
        <input type="submit" value="Pay by Credit Card">
</form>
```

2.2 Authorisation request parameter table

Field	Name	Size	Type	Mandatory	Description
Note: None of the parameters may contain an ampersand or an equal sign.					
a	p1	10	Alphanumeric	**Yes**	**VCS Terminal ID** allocated by VCS.
b	p2	25	Alphanumeric	**Yes**	**Unique Transaction Reference Number** with no spaces and no special characters, generated by the merchant. This reference number MUST ONLY BE USED ONCE. If for some reason the merchant did not get a response, then re-try the transaction with the same reference number. The VCS system will return the response received from the bank the first time the transaction was presented. VCS will not re-try the authorisation request if it has already been presented to the bank and VCS received a bank response. VCS will merely return the bank response on the system with the duplicate indicator. If the merchant received a response, but it was declined, and now wishes to try again, then the reference number must be changed. See p2 logic diagram on the last page of this document. The reference number in the transaction table can be a maximum length of 25 chars. The maximum length of reference numbers for RECURRING transactions is 15 chars. For RECURRING transactions VCS adds -yymmdd to the reference number to make the references unique and a, b, etc. for the retry attempts. Therefore VCS only uses the left 15 chars of the reference number for RECURRING transactions.
c	p3	50	Alphanumeric	**Yes**	**Description of Goods** is a short description generated by the merchant.
d	p4	10 include decim. point	Numeric	**Yes**	**Transaction Amount** with a decimal point, calculated by the merchant. If the amount does not include the decimal point, VCS will assume one at the end of the amount, i.e. 10 is 10.00.
e	p5	3	Alpha	No	**ISO Currency**, i.e. zar, usd, gbp, etc. If no currency received, then the VCS system will default to the merchant's default currency.

<table>
<tr><td colspan="7">Authorisation request parameter table – recurring parameters</td></tr>
<tr><th>Field</th><th>Name</th><th>Size</th><th>Type</th><th>Mandatory</th><th colspan="2">Description</th></tr>
<tr><td colspan="7"><b>Note:</b> Only include the recurring parameters if the transaction should re-occur. If the merchant does not want the transaction to re-occur then exclude the name/value pair completely.</td></tr>
<tr><td>f</td><td>p6</td><td>2</td><td>Alphanumeric</td><td>No</td><td colspan="2"><b>Occur Count</b>, 1 – 99 or U for an unlimited number of occurrences.
If Occur Frequency=O then Occur Count=1</td></tr>
<tr><td rowspan="8">g</td><td rowspan="8">p7</td><td rowspan="8">1</td><td rowspan="8">Alpha</td><td rowspan="8">No</td><td colspan="2"><b>Occur Frequency</b>.</td></tr>
<tr><td>D</td><td>Daily</td></tr>
<tr><td>W</td><td>Weekly</td></tr>
<tr><td>M</td><td>Monthly</td></tr>
<tr><td>Q</td><td>Quarterly (3-monthly)</td></tr>
<tr><td>6</td><td>Bi-annually (6-monthly)</td></tr>
<tr><td>Y</td><td>Annually</td></tr>
<tr><td>O (Oscar not Zero)</td><td>On Demand, to store card details in the recurring system after a valid approved authorisation but not to generate further automated recurring transactions. The merchant can request a manual (Virtual Terminal) or host to host On Demand authorisation using the stored card details. See On Demand host to host authorisation request for host to host specifications.</td></tr>
<tr><td>k</td><td>p11</td><td>255</td><td>Alphanumeric</td><td>No</td><td colspan="2"><b>Occurrence E-mail Address</b>.
If e-mail address included then VCS will send a transaction receipt to the cardholder after each occurrence. If this e-mail address is omitted then the e-mail address captured on the payment page will be used to populate the recurring e-mail parameter.</td></tr>
<tr><td>m</td><td>p13</td><td>6.2</td><td>Numeric</td><td>No</td><td colspan="2"><b>Occur Amount</b>, with a decimal point.
If decimal point not included then VCS will assume one at the end of the amount, i.e. 10 is 10.00. If this amount is omitted then the actual amount will be used by default.</td></tr>
<tr><td>o</td><td>NextOccurDate</td><td>10</td><td>Numeric and /</td><td>No</td><td colspan="2"><b>Next Occurrence Date</b>.
This is the date that the next occurrence of this transaction will be presented irrespective of what the occurrence frequency is. This date must be greater than the date that the transaction is presented. Format: ccyy/mm/dd.
If the next occur date is omitted then the first authorisation date plus occur frequency will be used.</td></tr>
</table>

<table>
<tr><td colspan="7">Authorisation request parameter table – optional parameters</td></tr>
<tr><th>Field</th><th>Name</th><th>Size</th><th>Type</th><th>Mandatory</th><th colspan="2">Description</th></tr>
<tr><td colspan="7"><b>Note</b>: If the optional parameters are not used, then exclude the name/value pair completely.</td></tr>
<tr><td>h</td><td>p8</td><td>10</td><td>Numeric</td><td>No</td><td colspan="2"><b>Cell phone Number</b> for SMS message.
VCS can send a message to a cell phone on any network.
Request Virtual Message registration from support@vcs.co.za.</td></tr>
<tr><td>i</td><td>p9</td><td>140</td><td>Alphanumeric</td><td>No</td><td colspan="2"><b>Message</b> for SMS.
This message will be sent to the above cell phone.
VCS will add the authorisation response received from the bank after this message.
Include only if registered Virtual Message user.</td></tr>
<tr><td>j</td><td>p10</td><td>255</td><td>Alphanumeric</td><td>No</td><td colspan="2"><b>URL for Cancelled Transactions</b>.
If the cardholder presses the cancel button on the VCS credit card entry page, VCS will return him to this URL.
VCS will return p1,p2,m_1 to m_10 but they are attached to the URL so:
http://xxx.xxx.xxx/yyy.asp?p1=zzzz&p2=1234&m_1=&m_2= etc.
If this URL is omitted the cardholder will be returned to the previous page by default.</td></tr>
<tr><td rowspan="3">l</td><td rowspan="3">p12</td><td rowspan="3">1</td><td rowspan="3">Alpha</td><td rowspan="3">No</td><td colspan="2"><b>Delayed Settlement</b>.</td></tr>
<tr><td>Y</td><td>Settlement delayed until manually released by merchant.</td></tr>
<tr><td>N</td><td>Settle today - automatic process.
The default option.</td></tr>
<tr><td rowspan="3">n</td><td rowspan="3">Budget</td><td rowspan="3">1</td><td rowspan="3">Alpha</td><td rowspan="3">No</td><td colspan="2"><b>Budget Period Allowed</b>.</td></tr>
<tr><td>Y</td><td>Budget is allowed, the default option.</td></tr>
<tr><td>N</td><td>Budget period is not allowed.</td></tr>
<tr><td>p</td><td>CardholderEmail</td><td>255</td><td>Alphanumeric</td><td>No</td><td colspan="2"><b>Cardholder E-mail Address</b>.
If e-mail address included then the cardholder e-mail address field on the VCS credit card payment page will be filled in, however the cardholder will be able to change it.
VCS will send a VCS credit card transaction receipt to this e-mail address.</td></tr>
</table>

<table>
<tr><td colspan="6">Authorisation request parameter table – optional parameters continued</td></tr>
<tr><th>Field</th><th>Name</th><th>Size</th><th>Type</th><th>Mandatory</th><th>Description</th></tr>
<tr><td colspan="6"><b>Note</b>: If the optional parameters are not used, then exclude the name/value pair completely.</td></tr>
<tr><td>q</td><td>Hash</td><td>32</td><td>Alphanumeric</td><td>No</td><td><b>MD5 hash value</b> provides a method for VCS to detect whether the parameters that the merchant sent to VCS have been tampered with, after leaving the merchant’s site and before arriving at the VCS site.
The merchant calculates the hash value from the normal parameters plus a secret (shared with VCS) and then send the hash value to VCS along with the normal parameters. VCS performs the same calculation again using the shared secret and if the two hash values are different then the data has been modified between the merchant sending it and VCS receiving it.
Hash types:
1 - <b>PAM hash value</b>
Request hash activation from support@vcs.co.za.
Set the PAM field inside Virtual Terminal, see Merchant Settings.
Concatenate all the parameters and the PAM value and perform an MD5 hash calculation.
VCS will take the same values from the incoming message and add the PAM from the VCS merchant record and perform an MD5 hash calculation.
2 - <b>MD5 hash value</b>
Forward MD5 key to support@vcs.co.za.
Concatenate all the parameters and the MD5 key value and perform an MD5 hash calculation.
VCS will take the same values from the incoming message and add the MD5 key value from the VCS merchant record and perform an MD5 hash calculation.
If the VCS hash value and the merchant hash value does not match VCS will reject the transaction with “MD5 Hash mismatch”.</td></tr>
<tr><td>z</td><td>m_1</td><td>100</td><td>Alphanumeric</td><td>No</td><td><b>Merchant Parameters</b> m_1 to m_10.
The m_ fields are merchant pass-through variables. Can be set to anything and will be returned with the response.</td></tr>
</table>

3. AUTHORISATION RESPONSE

The real-time authorisation results can be processed / displayed in the following ways:

3.1.1 VCS default response page

Utilise the VCS default authorisation response page if no additional interaction with the merchant's website is required.

3.1.2 Merchant response pages

The merchant creates two additional pages to receive the response and parameters VCS returns.
For an APPROVED response, VCS redirects the browser to the merchant's approved URL: http: or https: //merchant-approved-page-url.
For a NOT APPROVED response, VCS redirects the browser to the merchant's declined URL: http: or https: //merchant-not-approved-page-url.

The merchant configures his VCS merchant settings by going to https://www.vcs.co.za > Admin Login > Virtual Terminal > login > Merchant Administration > 3. Vcs Interfacing (page 1).

- Load the merchant's approved and declined URLs.
- Activate the correct Http method (response to browser).

If the merchant setting for the Http method is set to **GET**, then VCS imbeds the parameters into the URL. See the authorisation response example below.
If the merchant setting for the Http method is set to **POST,** the parameters will be imbedded into the HTTP header.
If the merchant setting for the Http method is set to **FETCH&POST** or **FETCH&GET** then VCS will request the approved or declined page from the merchant and send it to the cardholder's browser. If VCS "fetches" the pages from the merchant and deliver them then the merchant cannot use any relative addressing to his pages and images etc.; the merchant must use absolute URLs on his response pages.

3.1.3 Call-back function

The merchant can use the VCS default or merchant response pages to display the authorisation response and the call-back function to receive the parameters VCS returns.

The merchant creates a web page for receiving notification of all transactions processed named the call-back page.

In addition to the normal response to the merchant's response pages, VCS will also call the merchant's call-back page with the same authorisation response parameters in a non-browser dependant way.
This means that even if the cardholder closes the browser early or something goes wrong on the cardholder side, VCS will still notify the merchant of the result of the transaction.
The merchant's call-back page can then do database updates, send confirmation emails etc. irrespective of whether the cardholder's browser session ended prematurely or not.

VCS will dispatch failed call-back notifications to the correspondence email address for failed delivery attempts with the reason for the failure.

The merchant must always return <CallbackResponse>TagValue</CallbackResponse> to VCS when VCS invokes the call-back URL.
Where the TagValue must be the *Constant*: **Accepted** or else *The Reason* for **Failure**.

Authorisation response 3.1.3 Call-back Function – continued

Examples:
<CallbackResponse>Accepted</CallbackResponse> - if no technical difficulties were experienced.
Or <CallbackResponse>Failed</CallbackResponse> - if not Accepted.

VCS will continue delivery attempts to the call-back URL if the *Constant*: **Accepted** is not returned as the <CallbackResponse> tag Value.

The call-back page should simply pick up the parameters VCS returns, store them and respond with 'Accepted'. The merchant reconciliation of call-back data can then be done using the stored values.

For example right at the end of the call-back page write the string - in classic ASP it will look like this:

```
Response.Write "<CallBackResponse>Accepted</CallBackResponse>"
Response.End
```

Please note that the call-back page will be invoked after **EVERY** authorization, which includes manual transactions captured via Virtual Terminal, batch processing and recurring transactions.

To activate the call-back function go to https://www.vcs.co.za > Admin Login > Virtual Terminal > login > Merchant Administration > 6. Callback Settings > set Do Auth Callback to *Yes* > load the call-back URL in the approved and declined URL fields > set Callback Protocol to Http or Https > select Callback Method > set the Response Format > click the Modify button. The Do Markup Callback and Markup URL settings apply to section 5.2.1 Reporting host to host settlement mark-up.

3.2 Authorisation response example

```
Request.QueryString("p1") 'VCS Terminal ID
Request.QueryString("p2") 'Reference Number
Request.QueryString("p3") 'Response
Request.QueryString("p4") 'Constant: Duplicate (if applicable)
Request.QueryString("p5") 'Card Holder Name
Request.QueryString("p6") 'Amount
Request.QueryString("p7") 'Card Type
Request.QueryString("p8") 'Description of Goods
Request.QueryString("p9") 'Cardholder email Address
Request.QueryString("p10") 'Budget Period
Request.QueryString("p11") 'Expiry Date
Request.QueryString("p12") 'Response Code
Request.QueryString("pam") 'Authentication Message (stored at VCS)
Request.QueryString("m_1") 'Merchant Parameter
Request.QueryString("m_2") 'Merchant Parameter
Request.QueryString("m_3") 'Merchant Parameter
Request.QueryString("m_4") 'Merchant Parameter
Request.QueryString("m_5") 'Merchant Parameter
Request.QueryString("m_6") 'Merchant Parameter
Request.QueryString("m_7") 'Merchant Parameter
Request.QueryString("m_8") 'Merchant Parameter
Request.QueryString("m_9") 'Merchant Parameter
Request.QueryString("m_10") 'Merchant Parameter
Request.QueryString("CardHolderIpAddr") 'The browser's IP Address
Request.QueryString("MaskedCardNumber") 'Masked Card Number
Request.QueryString("TransactionType") 'Transaction Type
Request.QueryString("hash") 'Hash value (if hashing is selected)
```

3.3 Authorisation response parameter table

Name	Size	Type	Description
p1	4	Alphanumeric	**VCS Terminal ID**, allocated by VCS.
p2	25	Alphanumeric	**Unique Transaction Reference Number** from the incoming request.
p3	30	Alphanumeric	**Authorisation Response** returned by the bank. For an APPROVED bank response expect: Characters 1 – 6: The first 6 characters contain the bank's alphanumeric **authorisation number**, e.g. 123456 Characters 7 – 16: From character 7 the constant word **APPROVED**, left justified right space filled. For a NOT-APPROVED bank response expect: Characters 1 – 16: The bank's **reason for the declined transaction**, e.g. Not sufficient funds.
p4	9	Alpha	The word **Duplicate** if this transaction has been presented to us before and we are merely returning the response from the first transaction.
p5	30	Alphanumeric	**Name** entered by the cardholder on the VCS authorisation page.
p6	6.2	Numeric	**Amount** authorised by the bank.
p7	10	Alpha	**Card Type** selected by the cardholder from dropdown menu on the VCS page: MasterCard, Visa, Amex or Diners.
p8	50	Alphanumeric	**Description of Goods** from the incoming request.

Authorisation response parameter table – continued

Name	Size	Type	Description
p9	255	Alphanumeric	**Cardholder e-mail address** if entered on the VCS authorisation page.
p10	2	Numeric	**Budget Period** entered by the cardholder on the VCS authorisation page. 00 = straight
p11	4	Numeric	**Expiry Date** entered by the cardholder on the VCS authorisation page – format yymm.
p12	1 or 2	Alphanumeric	**Authorisation Response Code** received from the bank, e.g. 00 = Approved or 0 = Approved (Nedbank acq.) 05 = Do not honour etc.
pam	50	Alphanumeric	**PAM** - Personal Authentication Message, a security feature to confirm that the response is from VCS. The merchant enters the Merchant PAM in his Virtual Terminal merchant settings and VCS returns that PAM with the response.
m_1	100	Alphanumeric	**Merchant Parameter**(s) returned, if applicable.
CardHolderIpAddr	15	Numeric	**Cardholder Browser IP Address**, e.g. 41.177.38.1
MaskedCardNumber	16	Numeric	**Masked Card Number**, entered by the cardholder on the authorisation page, e.g. ************1234.
TransactionType	13	Alpha	**Transaction Type**, the possible values are Authorisation, Settlement or Refund. For an authorisation response we will return &TransactionType=Authorisation. For a settlement response we will return &TransactionType=Settlement. For a refund response we will return &TransactionType=Refund.
hash	32	Alphanumeric	**Hash Parameter**, if hashing is activated VCS will return an MD5 hash of the output parameters and the shared secret.

4. ON DEMAND HOST TO HOST AUTHORISATION REQUEST

The original authorisation request must include the Occur Frequency parameter of “O” for On Demand. This will cause our system to insert an On Demand transaction into the recurring transactions table once the original authorisation request has been approved. When requesting an On Demand authorisation, the VCS system will retrieve the cardholder’s details from the original transaction and use them again for the new immediate authorisation request and return the approved or not-approved authorisation response.

The following code is used to request an On Demand authorisation.

You need to create an HTML "POST" to our website as shown in the example below. The actual method of creation of the message and the request are not important except that the method must be POST and the message must be a properly formed XML Document.

VBScript example using Microsoft MsXml4

```
Dim xmlServerHttp
Dim xmlServerStatus
Dim XmlServerResponse

Set xmlServerHttp = Server.CreateObject("MsXml2.ServerXmlHTTP.4.0")

xmlServerHttp.open "POST","https://www.vcs.co.za/vvonline/ccxmldemand.asp",False
xmlServerHttp.setRequestHeader "Content-Type","application/x-www-form-urlencoded"
xmlServerHttp.send “xmlmessage=” & XmlDocument
xmlServerStatus = xmlServerHttp.status

if xmlServerStatus = "200" then
        xmlServerResponse = xmlServerHttp.responseText
        Response.Write (xmlServerResponse)
Else
        Response.Appendtolog ".xmlServer status is " & xmlServerStatus
end if

set xmlServerHttp = nothing
```

Where XmlDocument = the Xml Document below.

4.1 On Demand authorisation request example

```
<?xml version='1.0' encoding='UTF-8'?>
        <DemandRequest>
                <UserId>XXXX</UserId>
                <Reference>abc123</Reference>
                <Description>Test description of goods</Description>
                <Amount>5.00</Amount>
                <m_1>m1</m_1>
                <m_2>m2</m_2>
                <m_3>m3</m_3>
                <m_4>m4</m_4>
                <m_5>m5</m_5>
                <m_6>m6</m_6>
                <m_7>m7</m_7>
                <m_8>m8</m_8>
                <m_9>m9</m_9>
                <m_10>m10</m_10>
        </DemandRequest>
```

4.2 On Demand authorisation request parameter table

Name	Size	Type	Mandatory	Description
Note: None of the parameters may contain an ampersand or an equal sign.				
UserId	10	Alphanumeric	Yes	**VCS Terminal ID**.
Reference	25	Alphanumeric	Yes	**Reference Number** from the original authorisation request. This reference must match the On Demand recurring table's reference number. We add -yymmddhh to the original reference number to make the On Demand references unique. Therefore only one On Demand authorisation per hour per card can be processed, more than one will result in a duplicate authorisation response. We only use the left 15 chars of the original reference number for the On Demand transaction.
Description	50	Alphanumeric	Yes	**Description** of Goods / Product.
Amount	6.2	Numeric	Yes	**Transaction Amount**, specify the amount for the new On Demand transaction.
m_1	100	Alphanumeric	No	**Merchant Parameters** m_1 to m_10. The m_ fields are merchant variables that echo. Can be set to anything and will be returned with the response.

4.3 On Demand authorisation response example

```
<?xml version="1.0" ?>
      - <AuthorisationResponse>
              <UserId>XXXX</UserId>
              <Reference> abc123-yymmddhh</Reference>
              <Response>123456APPROVED</Response>
              <AdditionalResponseData />d
              <CardholderName>Name</CardholderName>
              <Amount>5.00</Amount>
              <DescrOfGoods>Test description of goods</DescrOfGoods>
              <CardholderEmail>email@email.com</CardholderEmail>
              <BudgetPeriod>00</BudgetPeriod>
              <ExpiryDate>1001</ExpiryDate>
              <ResponseCode>00</ResponseCode>
              <MerchPam>x</MerchPam>
              <m_1>x</m_1>
              <m_2>x</m_2>
              <m_3>x</m_3>
              <m_4>x</m_4>
              <m_5>x</m_5>
              <m_6>x</m_6>
              <m_7>x</m_7>
              <m_8>x</m_8>
              <m_9>x</m_9>
              <m_10>x</m_10>
              <MaskedCardNumber>************1234</MaskedCardNumber>
       </AuthorisationResponse>
```

4.4 On Demand authorisation response parameter table

<table>
<tr><th>Parameter</th><th>Max</th><th>Type</th><th colspan="2">Comments</th></tr>
<tr><td>UserId</td><td>4</td><td>Alphanumeric</td><td colspan="2"><b>VCS Terminal ID</b></td></tr>
<tr><td>Reference</td><td>25</td><td>Alphanumeric</td><td colspan="2"><b>Reference Number</b> from the original authorisation request plus the -yymmddhh that we added to the original reference number to make the On Demand references unique, e.g. Inv00001dup-09031510</td></tr>
<tr><td rowspan="4">Response</td><td rowspan="4">30</td><td rowspan="4">Alphanumeric</td><td colspan="2"><b>Authorisation Response</b> returned by the bank.</td></tr>
<tr><td>Characters 1-6</td><td>For <b>approved</b> transactions the first 6 characters contain the bank’s alphanumeric authorisation number.</td></tr>
<tr><td>Characters 7-16</td><td>For <b>approved</b> transactions expect from character 7 the constant word APPROVED, left justified right space filled.</td></tr>
<tr><td>Characters 1-16</td><td><b>Not approved</b> transactions, contain the bank’s reason for the declined authorisation request, e.g. Not sufficient funds.</td></tr>
<tr><td>AdditionalResponseData</td><td></td><td>Alphanumeric</td><td colspan="2">The word <b>Duplicate</b> if this transaction has been presented to us before and we are merely returning the response from the first transaction.</td></tr>
<tr><td>CardholderName</td><td>30</td><td>Alphanumeric</td><td colspan="2">Returning the <b>Cardholder Name</b>.</td></tr>
<tr><td>Amount</td><td>6.2</td><td>Numeric</td><td colspan="2"><b>Amount</b> of the authorisation request.</td></tr>
<tr><td>DescrOfGoods</td><td>50</td><td>Alphanumeric</td><td colspan="2">Returning the <b>Description of Goods</b>.</td></tr>
<tr><td>CardholderEmail</td><td>255</td><td>Alphanumeric</td><td colspan="2">Returning the <b>Cardholder Email</b> address.</td></tr>
<tr><td>BudgetPeriod</td><td>2</td><td>Numeric</td><td colspan="2">Returning the <b>Budget Period</b>.</td></tr>
<tr><td>ExpiryDate</td><td>4</td><td>Numeric</td><td colspan="2">Returning the <b>Expiry Date</b> – format yymm</td></tr>
<tr><td>ResponseCode</td><td>2</td><td>Alphanumeric</td><td colspan="2">Authorisation <b>Response Code</b> received from the bank.</td></tr>
<tr><td>MerchPam</td><td>50</td><td>Alphanumeric</td><td colspan="2"><b>Personal Authentication Message,</b> a security feature to confirm that the response is from VCS. The merchant enters the Merchant PAM in his Merchant Settings and VCS returns that PAM with the response.</td></tr>
<tr><td>m_1</td><td>100</td><td>Alphanumeric</td><td colspan="2"><b>Merchant Parameter(s)</b> m_1 to m_10 returned.</td></tr>
<tr><td>MaskedCardNumber</td><td>16</td><td>Numeric</td><td colspan="2">Returning <b>Masked Card Number,</b> e.g. ************1234</td></tr>
</table>

5. REPORTING

5.1 Daily reports

Authorisation Report – an audit trail of the previous day's authorisation attempts.

Failed Authorisation Report – a list of the previous day's not-approved authorisation attempts.

Outstanding Settlement Report – to inform the merchant of transactions that's waiting for settlement confirmation from bank. Settlement can be delayed by week-ends, public holidays or by the bank's risk management security checks.

Settlement Report – this report is generated from the bank's daily settlement mark-up file.
It lists the transactions that received settlement confirmation / mark-up from the bank.
The settlement report reconciles with the batch payment that reflects on the merchant's bank statement.

5.2 Reporting format

Email - HTML email reports are dispatched to the merchant with the report data attached as a comma-delimited .txt file. The VCS back office, Virtual Terminal, provides the ability to the merchant to select which reports he wants to or does not want to receive.

FTP files - VCS can provide FTP files instead of email reports; request the FTP output file specifications from support@vcs.co.za.

Host to host settlement mark-up - VCS receives settlement mark-up data from the banks / acquiring institutions on a daily basis.
This data confirms the settlement of approved transactions.
VCS can post the settlement parameters to the merchant's mark-up URL to provide host to host confirmations of settlements.
To activate the mark-up call-back function refer to the Merchant Settings section of this document.

5.2.1 Reporting host to host settlement mark-up example

Where the Merchant Setting's call-back response format has been set to Name Value Pairs (ccForm – p1, p2...) we will return the following parameters:

```
p1=XXXX
&p2=REF000001
&p6=123.45
&MarkupType=Debit
&MarkupReference=0010000001
&MarkupDateTime=2008/10/13+16:31:21
&pam=my+dog+skip
&m_1=fred1
&m_2=fred2
&m_3=fred3
&m_4=fred4
&m_5=fred5
&m_6=fred6
&m_7=fred7
&m_8=fred8
&m_9=fred9
&m_10=fred10
&MaskedCardNumber=************0002
```

5.2.2 Reporting host to host settlement mark-up parameter table

Name	Size	Type	Description
p1	4	Alphanumeric	**VCS Terminal ID,** allocated by VCS.
p2	25	Alphanumeric	**Unique Transaction Reference Number** from the authorisation request, allocated by the merchant.
p6	6.2	Numeric	**Settlement Amount**. For **sales** the amount will not contain a sign indicator e.g. &p6=123.45 For **refunds** the amount will contain a negative sign indicator e.g. &p6=-123.45
MarkupType	6	Alpha	**Transaction Type**. For **sales** the MarkupType will be ‘Debit’ e.g. &MarkupType=Debit For **refunds** the MarkupType will be 'Credit' e.g. &MarkupType=Credit
MarkupReference	16	Alphanumeric	**Mark-up Reference Number** allocated by the bank.
MarkupDateTime	19	Alphanumeric	**Date and time** that settlement was processed. Format: ccyy/mm/dd hh:mm:ss (URL encoded)
pam	50	Alphanumeric	**PAM - Personal Authentication Message,** a security feature to confirm that the call is from VCS. The merchant enters the Merchant PAM in his Virtual Terminal merchant settings and VCS returns that PAM with the call.
m_1	100	Alphanumeric	**Merchant Parameter(s)** returned, if applicable.
MaskedCardNumber	16	Numeric	**Masked Card Number** of the card that was debited / credited, e.g. ************1234.

6. MERCHANT SETTINGS

How to submit the approved & declined URLs, call-back URLs and PAM:

- Go to www.vcs.co.za.
- Admin Login > Virtual Terminal.
- Enter the user login name and password that was confirmed via the VCS application approved e-mail.
- Click the **Merchant Administration** link.
- Select **3. VCS Interfacing (page1)** from the drop down.
    - Enter merchant's website, approved & declined URLs.
    - Select the response to browser method (POST or GET).
    - The Referrer URL is an optional URL. It is used as a precautionary measure to prevent malicious interception of parameters between merchant's website and payment gateway.
- Select **4. VCS Interfacing (page2)** from the drop down.
    - Enter Merchant PAM for the MD5 hash value security feature.
- Select **6. Callback Settings** to activate the real-time authorisation call-back function and / or the daily settlement mark-up call-back.
    - To activate the call-back function set Do Auth Callback to Yes; enter call-back URLs; select protocol, method & format; click Modify.
    - To activate the daily settlement mark-up call-back set the Do Markup Callback to Yes; enter mark-up URL; select protocol, method and format; click Modify.

Forward the merchant's company logo (maximum banner size 750 x 150 pixels) in .gif or .jpg format to support@vcs.co.za. This logo will be displayed to the cardholder on the VCS credit card authorisation payment page.

7. TEST

New merchants loaded on the VCS system have access to the VCS Test platform.
We run a response generator that has some fixed but mostly random responses.

Test Card Number	CVC number & Expiry Date	Fixed simulated authorisation response
4242424242424242	Use any CVC number, e.g. 123. Use any valid expiry date.	123456Approved Where 123456 = any alphanumeric value
5454545454545454		123456Approved Where 123456 = any alphanumeric value
5221001010000024		Call
5221001010000032		Invalid Expiry
5221001010000040		~No Active Connection to Acquirer exists

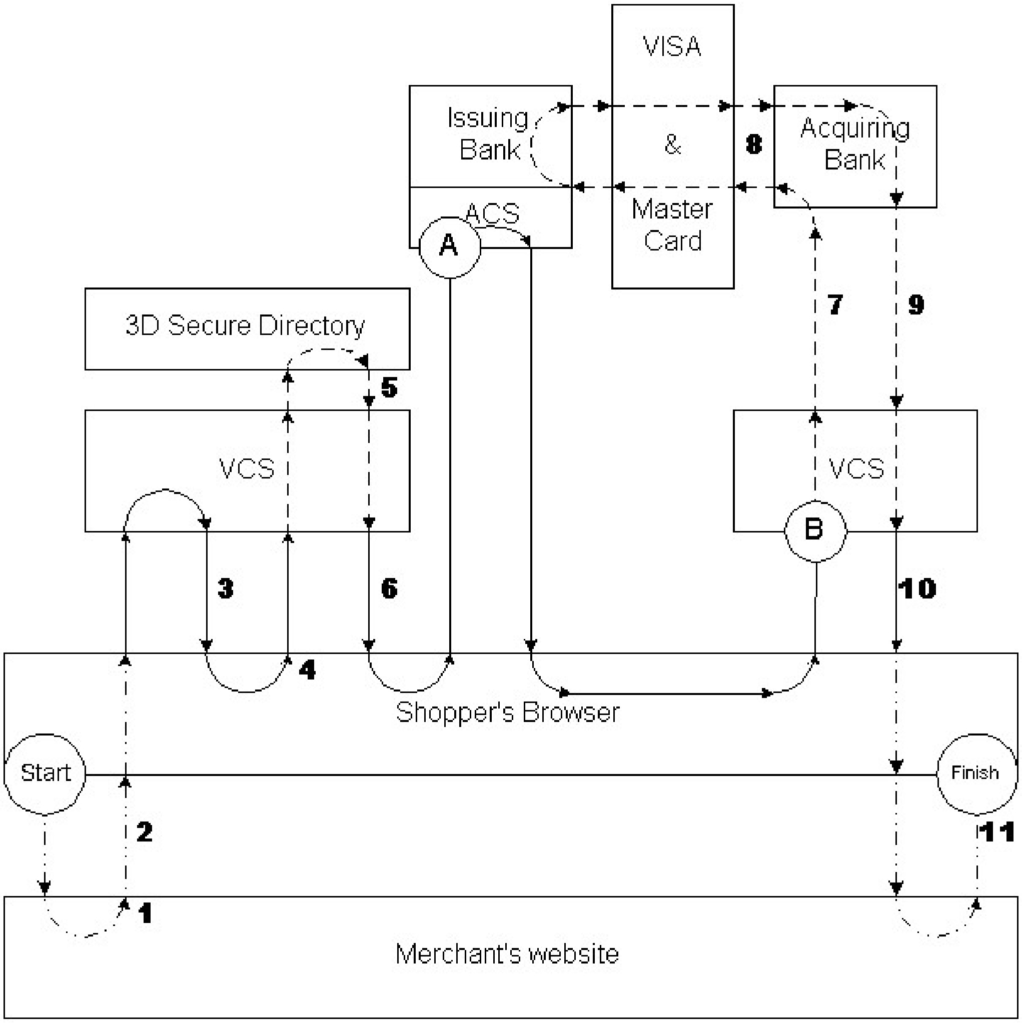
Any valid credit card number can be submitted to the test platform during the test phase because no real money is involved.
The following responses occur randomly with any other card number used.
"Invalid Terminal", "Declined", "Invalid Expiry", "Batch Full", "Call", "123456Approved"

Please ensure that sufficient testing has been completed before requesting activation as once a terminal has been activated it cannot be reset into Test status.

8. ACTIVATION

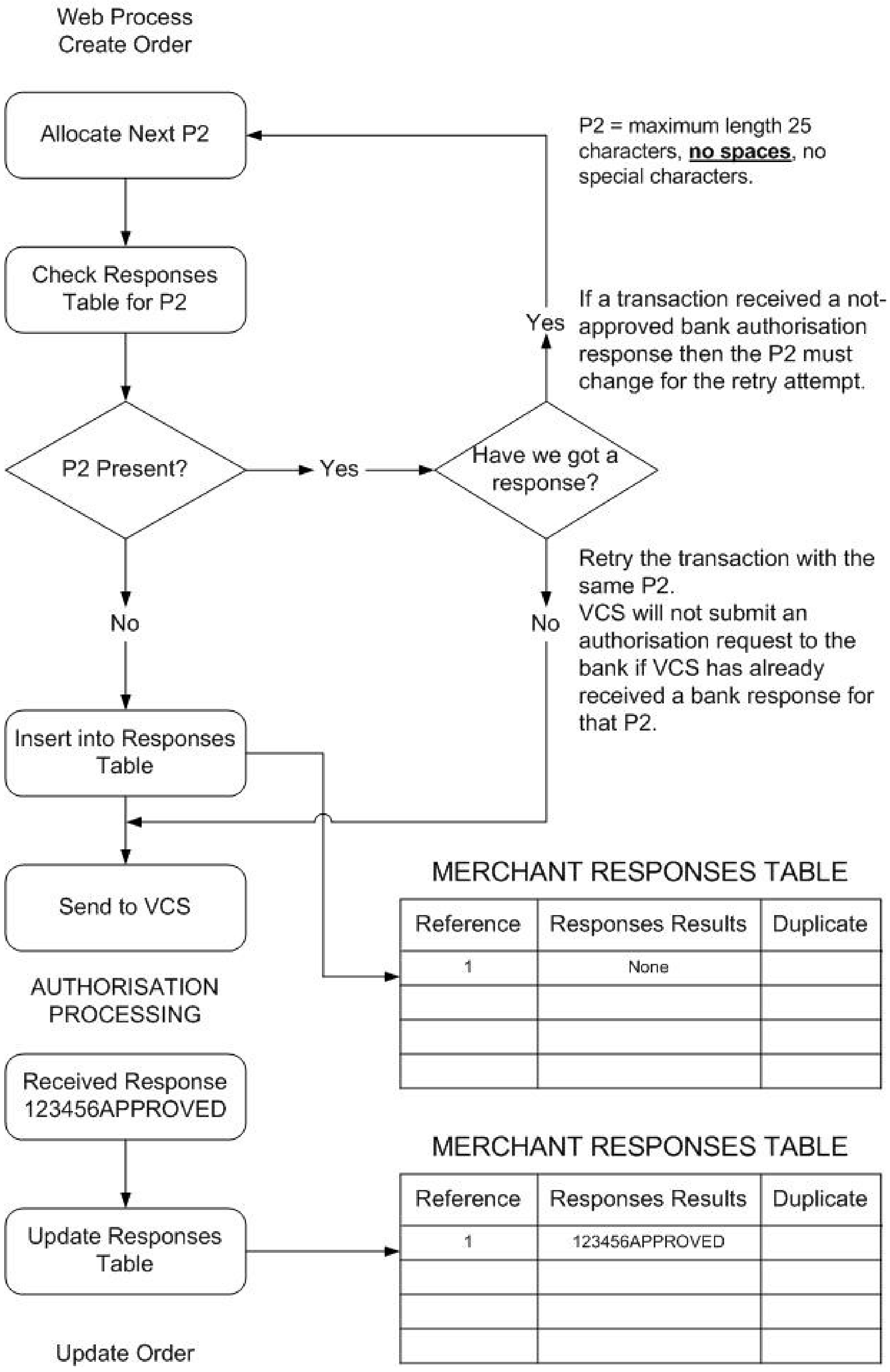
To enable "live" operation send an activation request by e-mail to support@vcs.co.za.
Please include your VCS terminal ID when requesting activation.

9. VERIFIED BY VISA / SECURE CODE TRANSACTION FLOW



1) The shopper selects the “Pay by Credit Card” option on the merchant’s website.
2) The merchant’s website instructs the shopper’s browser to redirect to VCS.
3) VCS sends out a secure credit card payment page (ccform) to the shopper’s browser.
4) The shopper submits his credit card details.
5) VCS requests the ACS (Authentication Control Server) address from the 3D secure directory.
6) VCS instructs the shopper’s browser to verify itself at A and to return with the answer to B.
7) If the answer = “Yes”, then VCS requests authorisation from the acquiring bank.
8) The acquiring bank requests authorisation from the issuing bank.
9) The acquiring bank responds to VCS.
10) VCS instructs the shopper’s browser to fetch the merchant’s response page from the merchant’s website.
11) The merchant’s response page is displayed to the shopper.

10. P2 - UNIQUE REFERENCE NUMBER LOGIC



P2 = maximum length 25 characters, **no spaces**, no special characters.

If a transaction received a not-approved bank authorisation response then the P2 must change for the retry attempt.

Retry the transaction with the same P2.
VCS will not submit an authorisation request to the bank if VCS has already received a bank response for that P2.

MERCHANT RESPONSES TABLE

Reference	Responses Results	Duplicate
1	None	

MERCHANT RESPONSES TABLE

Reference	Responses Results	Duplicate
1	123456APPROVED	