Virtual
card services

# VCSPAY

## INTERFACING SPECIFICATION

VIRTUAL CARD SERVICES

Rivonia Business Centre
377 Rivonia Boulevard, Rivonia
2128
Tel +27 11 593 2340
Fax +27 86 612 1435
sales@vcs.co.za

## TABLE OF CONTENTS

## 1. INTRODUCTION

The purpose of this document is to provide a web developer with the information necessary 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 site to divert the browser to VCS.

The transaction flow is as follows:

- Once the customer has completed the shopping process the merchant's web site must display a button showing "Proceed to Payment".

- When the customer clicks the "Proceed to Payment" button the merchant's web site must divert the customer's browser to VCS passing a few parameters.

- The VCS web site forces the browser into a secure mode and then displays all the payment options offered by the merchant.

- The customer selects which payment method they wish to use.

- VCS displays a form requesting the necessary information for the payment method chosen by the customer.

- If "Credit Card" is chosen a form is displayed requesting entry of the cardholder's information.
  The cardholder enters their information and presses "Pay".

- VCS performs a lookup in the MasterCard / VISA 3D Secure directory, and if necessary, performs the 3D Secure authentication process.

- VCS then connects to the merchant's acquiring bank and requests authorisation for the transaction from the issuer of the card.

- VCS diverts the cardholder to the merchant's web site, to an "Approved", or a "Declined" page, depending on the response from the bank.
  VCS can also enter the transaction into a "Call-back" queue which operates independently of the browser and notifies the merchant's web site of the result of the transaction repeatedly until it is acknowledged as being accepted by the merchant's web site.

## 2. AUTHORISATION REQUEST

The merchant's check out page must contain a form with a submit button to "POST" the cardholder's browser to the VCS website. Only the first four parameters (p1, p2, p3 and p4) and the MD5Hash are mandatory. The rest of the parameters are optional.

### 2.1 EXAMPLE HTML CODE

```
<form method="POST" action="https://www.vcs.co.za/vvonline/vcspay.aspx">
        <input type="hidden" name="p1" value="VCS Terminal ID">
        <input type="hidden" name="p2" value="Transaction Reference Number">
        <input type="hidden" name="p3" value="Description of Goods">
        <input type="hidden" name="p4" value="Transaction Amount">
        <input type="hidden" name="Hash" value="Hash">
        <input type="submit" value="Proceed to Payment">
</form>
```

### 2.2 AUTHORISATION REQUEST PARAMETER TABLE

| NAME | SIZE | DESCRIPTION / PARAMETER VALUE |
|---|---|---|
| p1 | 10 | **VCS Terminal Id** - Mandatory - *Alphanumeric*<br><br>Allocated by VCS |
| p2 | 25 | **Unique Transaction Reference Number** – Mandatory – *Alphanumeric*<br><br>Generated by the merchant, with maximum length of 25 chars, no spaces and no special characters.<br>The reference number MUST ONLY BE USED ONCE for each unique transaction. If for some reason merchant did not receive a response, then retry the transaction with the same reference number. Should the transaction have reached the VCS system and been processed then VCS 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 has received a bank response. VCS will simply return the original bank response with the duplicate indicator set. When generating a payment reference number it is recommended that the merchant's order number is included in the reference. If the merchant received a declined response and wishes to try again, then the reference number must be changed.<br>For RECURRING transactions VCS truncates the reference number after 15 chars and appends a sequence number on each occurrence to make the recurring references unique.<br>Note: refrain from using the "_" in referencing. During instant EFT processing the bank's translate the "_" to "//". |

| | | |
|---|---|---|
| p3 | 50 | **Description of Goods** – Mandatory - *Alphanumeric*<br><br>A short description of the goods, generated by the merchant, and displayed to the cardholder during the payment process. |
| p4 | 6.2 | **Transaction Amount** – Mandatory – *Numeric and decimal point*<br><br>With a decimal point between Rand and cents, do not use a comma.<br>If a decimal point is not included then VCS will assume one at the end of the amount, i.e. 10 will be assumed to be 10.00. |
| p5 | 3 | **ISO Currency Code** - *Alpha*<br><br>The currency of merchant acquiring bank, i.e. ZAR, BWP, NAD.<br>If no currency code is specified then the system will default to the merchants default currency. |
| p6 | 2 | **Occurrence Count** - *Alphanumeric*<br><br>***1*** - ***99*** or ***U*** for an unlimited number of occurrences.<br>If "Occur Frequency=O" then occur count must equal 1.<br><br>Include p6 only if the transaction should re-occur. |
| p7 | 1 | **Occurrence frequency** - *Alphanumeric*<br><br>***D*** for daily occurrence<br>***W*** for weekly occurrence<br>***M*** for monthly occurrence<br>***Q*** for quarterly (3-monthly) occurrence<br>***6*** for bi-annual (6-monthly) occurrence<br>***Y*** for annual occurrence<br><br>***O*** for on-demand transactions. By including this indicator VCS will store the card details in the recurring system, if the initial transaction is approved. A new transaction will not be generated unless an on-demand request is sent to VCS.<br><br>Include p7 only if the transaction should re-occur. |
| p11 | 255 | **Occurrence E-mail Address** - *Alphanumeric*<br><br>If an e-mail address is 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 entered on the payment page will be used to populate the recurring e-mail parameter.<br><br>Include only if the transaction should re-occur. |
| p13 | 6.2 | **Occurrence Amount** – *Numeric and decimal point* |

| | | |
|---|---|---|
| | | If a decimal point is not included then VCS will assume one at the end of the amount, i.e. 10 will be assumed to be 10.00.<br>If the occurrence amount is omitted then the actual amount (p4) will be used by default.<br><br>Include only if the transaction should re-occur. |
| NextOccurDate | 10 | **Next Occurrence Date** - *Numeric and /*<br><br>Format: ccyy/mm/dd.<br>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. If the next occurrence date is omitted then the date of first authorisation plus the frequency will be used to generate the next occurrence date.<br><br>Include only if the transaction should re-occur. |
| p8 | 10 | **Cell phone Number** - *Numeric*<br><br>VCS can send an SMS message to a cell phone on any network.<br><br>Only available to registered Virtual Message users. To apply go to www.virtualmessage.co.za and submit the online application form. |
| p9 | 140 | **Message for SMS** - *Alphanumeric*<br><br>This message will be sent to the above cell phone number. VCS will add the authorisation response received from the bank behind this message.<br><br>Include only if a registered Virtual Message user. |
| p10 | 255 | **URL for Cancelled Transactions** - *Alphanumeric*<br><br>If the cardholder clicks the cancel button on the VCS payment page, VCS will return the browser to this URL. VCS will return p1, p2, m_1 to m_10 but they are attached to the URL as following:<br>http://xxx.xxx.xxx/yyy.asp?p1=zzzz&p2=1234&m_1=&m_2= etc.<br>If this URL is omitted the browser will be returned to the previous page by default. |
| p12 | 1 | **Delayed Settlement** - *Alpha*<br><br>***Y*** to delay the settlement of the transaction until it is released. Either manually by the merchant using Virtual Terminal, or by a host to host call to the ccxmlsettle service.<br>***N*** to settle the transaction automatically, if approved. This is the default option. |

| | | |
|---|---|---|
| Budget | 1 | **Budget Period** - *Alpha*<br><br>***Y*** to allow the budget option on the payment page. This is the default option.<br>***N*** to hide the budget period option from the cardholder. |
| CardholderEmail | 255 | **Cardholder E-mail Address** - *Alphanumeric*<br><br>If the email address is included then the cardholder email address field on the VCS payment page will be filled in, however the cardholder will be able to change it. VCS will send a transaction receipt to this email address. |
| CardholderName | 50 | **Cardholder Name** - *Alphanumeric*<br><br>If this parameter is included the value will be inserted into the payment page and the cardholder will not need to enter their name.<br>If the cardholder selects the SID payment method the Cardholder Name will be passed as a parameter to the SID transaction. |
| Hash | 32 | **MD5 hash** - *Alphanumeric*<br><br>The MD5 hash provides a method for VCS to detect whether the parameters that the merchant sent to VCS have been tampered with. It also prevents transactions from being presented to VCS that did not originate within the merchant's environment.<br>If the VCS calculated hash value does not match the value in this field then VCS will reject the transaction with "MD5 Hash mismatch". |
| Mobile | 1 | **Mobile format** - *Alpha*<br><br>***Y*** to format the payment page for a small screen mobile device.<br>If omitted the default value will be ***N***. |
| Discount | 1 | **Mystery Discount** - *Alpha*<br><br>***Y*** to instruct VCS to reduce the amount from p4 by a mystery discount amount of between 0.01 and 0.99. The new amount will not be displayed to the purchaser, and will be returned in the response. The purchaser could then be asked what the final amount was in order to authenticate that they actually have access to that account. |
| UrlsProvided | 1 | **Override Virtual Terminal Response Settings Flag** - *Alpha*<br><br>Set to ***Y*** for the VCS system to ignore the primary response URL settings in Virtual Terminal. The ApprovedUrl and DeclinedUrl parameters must be included when this flag is incorporated. |
| ApprovedUrl | 255 | **URL for Approved Transactions** - *Alphanumeric* |

| | | |
|---|---|---|
| | | If UrlsProvided has been set to Y then this URL will be used as the primary response to browser URL for approved authorisations. |
| DeclinedUrl | 255 | **URL for Declined Transactions** - *Alphanumeric*<br><br>If UrlsProvided has been set to Y then this URL will be used as the primary response to browser URL for not-approved authorisations. |
| m_1 to m_10 | 100 | **Merchant Parameters** - *Alphanumeric*<br><br>m_1 to m_10 are merchant pass-through variables that can contain any value. They can be set to anything and will be returned with the response.<br><br>For sites that block access until payment has been made.<br>Set "m_1=hotspot", "m_2=a URL", "m_3=hotspot id".<br>VCS will do an HTTP POST to the m_2 URL, with the content of m_3 concatenated before a "name = value" pair "OpenUrl = the URL" that we need to re-direct the browser to. This will result in the following, for example:<br>"com=STA&cid=STA033&OpenUrl=https://3dsecureprd.fnb.co.za". Once you have opened access to this URL you must return an xml document containing <AccessOpened>Y</AccessOpened><br>VCS will then re-direct the browser to that URL to perform the 3D Secure authentication. When this has been completed the payment process will continue. |

Notes:

- None of the parameters may contain an ampersand or an equal sign.
- Refrain from using special characters in the parameter values. For example, during instant EFT processing the transaction may be blocked due to the special characters in the parameter values.
- Only include the optional recurring parameters if a recurring transaction should be generated automatically. If the merchant does not want the transaction to re-occur then exclude the name/value pair completely.
- If the optional parameters are not used, then exclude the name/value pair completely.

## 2.3 HASH FUNCTION

The merchant's web site calculates the MD5 HASH value from the normal parameters being passed to VCS plus a "secret", which can be a password, a text phrase or a key value. This value must have been previously communicated to VCS by sending the MD5 key to support@vcs.co.za, and it having been stored in the merchant record. The maximum size of MD5 key is 50 characters.

The merchant's web site then sends the calculated MD5 HASH value to VCS as an additional parameter along with the normal parameters.

VCS performs the same calculation, using the previously shared "secret". If the two hash values are different the transaction is rejected.

### 2.3.1 How to calculate the hash value

The merchant strings all the parameters, including the MD5key, into one variable i.e. concatenate all the parameters that you are about to send and the MD5 key value. Pass these to an MD5 hashing routine which will return a 32 character MD5 HASH value. Send MD5 HASH value to VCS as an additional parameter e.g. "&Hash=000987h5h6d462hgishr3jhg3j". The MD5 HASH can be passed to VCS in either upper or lower case. We will translate it to lower case before comparing it against the hash we calculate.

### 2.3.2 Concatenation sequence

If you pass any of the parameters from the following list then they must be included in your MD5 string and they must be included in the same sequence as specified below:
p1p2p3p4p5p6p7p8p9p10p11p12p13NextOccurDateBudgetCardholderEmailm_1
m_2m_3m_4m_5m_6m_7m_8m_9m_10Md5Key

E.g. where p1=xxxx, p2=1234, p3=Goods, p4=10.00 and the MD5 Key=Help then the variable that must be passed to the MD5 routine will look like this: xxxx1234Goods10.00Help

There should not be commas between the fields and if a field is not used then omit it completely.
Make sure that none of the parameters has been encoded i.e. if the parameter contains an ampersand then the value passed to the hashing routine should have "fred&joe" NOT "fred&joe".

### 2.3.3 Response concatenation sequence

The hash response concatenation sequence, to the merchant's response and call-back pages, is as follows:
p1p2p3p4p5p6p7p8p9p10p11p12pamm_1m_2m_3m_4m_5m_6m_7m_8m_9m_10CardHolderIpAddr
MaskedCardNumberTransactionTypeMd5Key

For example, the retrieval reference number, Uti, and 3D response parameters, are not included in the hash response concatenation sequence.

### 2.3. 4 Hash activation

Request hash activation from VCS by forwarding the MD5 key to support@vcs.co.za.

**2.3.5 Example of the code necessary to create the string to be passed to the MD5 function**

```
Imports System

Imports System.Security.Cryptography
Imports System.Text

Dim varMd5String
varMd5String = varP1 & varP2 & varP3 & varP4 & varP5 & varP6 & varP7 & varP8 & varP9 & varP10 &
varP11 & varP12 varMd5String = varMd5String & varP13 & varNextOccurDate & varBudget &
varCardholderEmail

varMd5String = varMd5String & m_1 & m_2 & m_3 & m_4 & m_5 & m_6 & m_7 & m_8 & m_9 & m_10
varMd5String = varMd5String & varMerchMd5Key

varMd5Hash = getMd5Hash(varMd5String)

‘ append the varMd5hash to the parameter string to be sent to VCS

‘
' HASH an input string and return the MD5 HASH as a 32 character hexadecimal string.

‘
Function getMd5Hash(ByVal input As String) As String

        ‘ Create a new instance of the MD5 object
        Dim md5Hasher As MD5 = MD5.Create()
        ‘ Convert the input string to a byte array and compute the hash.

        Dim data As Byte() = md5Hasher.ComputeHash(Encoding.Default.GetBytes(input))
        '       Create a new Stringbuilder to collect the bytes and create a string.

        Dim sBuilder As New StringBuilder()

        '       Loop through each byte of the hashed data and format each one as a hexadecimal
        string.
        Dim i As Integer

        For i = 0 To data.Length - 1 sBuilder.Append(data(i).ToString("x2"))

        Next i
        '       Return the hexadecimal string.

        Return sBuilder.ToString()

  End Function

End Module

'       This code example produces the following output: ed076287532e86365e841e92bfc50d8c
```

# 3. AUTHORISATION RESPONSE

## 3.1 PRIMARY AUTHORISATION RESPONSE DISPLAY AND PROCESSING

### 3.1.1 Response timing

Having re-directed the browser to VCS, the merchant's system should wait for a reasonable amount of time, e.g. 5-10 minutes, before assuming that no response has been received. This is due to the fact that if the customer chooses the "Credit card payment option" the 3DSecure process can take a few minutes, followed by the actual authorisation process; and if that fails the reversal process which takes time. If the customer selects MasterPass then there is an interaction with their mobile device and this process has a timeout value of 10 minutes.

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

### 3.1.2 VCS default response page

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

### 3.1.3 Merchant response pages

3.1.3.1 The merchant creates two additional pages to receive the response and parameters VCS returns. This is the primary immediate real time notification method, and cannot be turned off.

- 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

3.1.3.2 The merchant configures his VCS return URLs and response to browser method, by logging into Virtual Terminal > Merchant Administration > 3. Vcs Interfacing (page 1).

- Enter and save the approved and declined URLs.
- Activate the required Http Method (response – browser method).

  If the merchant setting for the Http method is set to GET, then VCS imbeds the parameters into the URL (query string).
  Use *Request.Querystring* to fetch the parameters.

  If the merchant setting for the Http method is set to POST, the parameters will be imbedded into the HTTP header.
  Use *Request.Form* to fetch the parameters.

  If the merchant elects to use the FETCH&POST, or FETCH&GET, VCS will fetch the pages from the merchant and deliver them to the browser. VCS will request the approved, or declined page, from the merchant's website, using an HTTP GET, or HTTP POST, and send the result returned to the cardholder's browser. In this case the merchant cannot use any relative addressing in the pages; the merchant must use absolute addressing in the response pages.

## 3.2 SECONDARY OPTIONAL CALL-BACK NOTIFICATION

The call-back is an optional method, which is not dependent on the customer's browser, where VCS stores the necessary information into a queue, and notifies the merchant's call-back page using a host-to-host call. Therefore the call-back response is not a real time response.
If the merchant activates the call-back, then in addition to the primary browser response, VCS will also call the merchant's call-back page, with the same authorisation response parameters. This means that if the cardholder closes the browser early, VCS will still notify the merchant of the result of the transaction.
In order to use the call-back function the merchant creates a web page for receiving the call-back, which is a notification of ALL transactions processed. The call-back will be invoked after EVERY authorisation, which includes manual authorisations captured via Virtual Terminal, batch processing and recurring transactions.
The correct way of handling the call-back is to write some code that can receive the parameters, and then to check whether the merchant has already received the response, and if so ignore it.
VCS will attempt to deliver the call-back five times. If the call is not accepted then VCS will notify the merchant of the failed call-back via email.

### 3.2.1 Call-back responses

The merchant must return <CallbackResponse>Accepted</CallbackResponse> to VCS when VCS invokes the call-back URL to acknowledge that the response was received.

The tag value must be the constant "Accepted".
If the tag was received and no technical difficulties were experienced, then VCS will not continue with the delivery attempts.

If the merchant does not respond with the <CallbackResponse> tag, or if the tag value is any value other than "Accepted", or if the call-back page is not reachable, or it produces errors, then VCS will retry the delivery five times and notify the merchant via email of the failed attempt.

### 3.2.2 Call back response example

Right at the end of the call-back page write a string in response - in classic ASP it will look like this:
Response.Write
"<CallBackResponse>Accepted</CallBackResponse>"Response.End

### 3.2.3 Activate the call-back function

- Go to https://www.vcs.co.za > click Virtual Terminal and login > click Merchant Administration > select Callback Settings from the dropdown selection
- Set Do Auth Callback to "Yes"
- Load the call-back URL in the approved and declined URL fields
- Set the Callback Protocol to Http or Https
- Select Callback Method
- Set the Response Format
- Click the Modify button

The Do Mark-up Callback and Mark-up URL settings are for host to host settlement mark-up, and do not apply to authorization responses.

### 3.3 AUTHORISATION RESPONSE EXAMPLE

If the merchant setting for the Http Method is set to POST:

Request.Form("p1") 'VCS Terminal ID
Request.Form("p2") 'Reference Number
Request.Form("p3") 'Response
Request.Form("p4") 'Constant: Duplicate (if applicable)
Request.Form("p5") 'Card Holder Name
Request.Form("p6") 'Amount
Request.Form("p7") 'Card Type
Request.Form("p8") 'Description of Goods
Request.Form("p9") 'Cardholder email Address
Request.Form("p10") 'Budget Period
Request.Form("p11") 'Expiry Date
Request.Form("p12") 'Response Code
Request.Form("pam") 'Authentication Message (stored at VCS)
Request.Form("m_1") 'Merchant Parameter
Request.Form("m_2") 'Merchant Parameter
Request.Form("m_3") 'Merchant Parameter
Request.Form("m_4") 'Merchant Parameter
Request.Form("m_5") 'Merchant Parameter
Request.Form("m_6") 'Merchant Parameter
Request.Form("m_7") 'Merchant Parameter
Request.Form("m_8") 'Merchant Parameter
Request.Form("m_9") 'Merchant Parameter
Request.Form("m_10") 'Merchant Parameter
Request.Form("CardHolderIpAddr") 'Browser IP Address
Request.Form("MaskedCardNumber") 'Masked Card Number
Request.Form("TransactionType") 'Transaction Type
Request.Form("hash") 'Hash value (if hashing is selected)
Request.Form("Uti") 'Unique transaction ID
Request.Form("threeDsecureEnrolled") 'Y/N
Request.Form("threeDsecureEci") 'ECI returned by the 3Ds process
Request.Form("threeDsecureXid") 'Transaction ID returned by the 3Ds process
Request.Form("threeDsecureCavv") 'CAVV returned by the 3Ds process

### 3.4 AUTHORISATION RESPONSE PARAMETER TABLE

| NAME | SIZE | DESCRIPTION |
|---|---|---|
| p1 | 10 | **VCS Terminal Id** - *Alphanumeric*<br><br>Allocated by VCS |
| p2 | 25 | **Unique Transaction Reference Number** - *Alphanumeric*<br><br>From the incoming authorisation request. |

| | | |
|---|---|---|
| p3 | | **Bank Authorisation Response** - *Alphanumeric*<br><br>For an APPROVED bank response expect, ***xxxxxx APPROVED***.<br>The first six characters contain the bank's alphanumeric authorisation<br>number, e.g. 123456<br>From character seven the constant word APPROVED, left justified right space filled.<br><br>For a NOT-APPROVED bank response expect the bank's reason for the declined transaction, e.g. Not sufficient funds. |
| p4 | 9 | **Duplicate Response Indicator** - *Alpha*<br><br>The word ***Duplicate*** if the transaction reference number has been presented to VCS before, and VCS is merely returning the response from the first transaction. |
| p5 | 30 | **Cardholder Name** - *Alphanumeric*<br><br>The name entered by the cardholder on the VCS payment page. |
| p6 | 6.2 | **Transaction Amount** - *Numeric*<br><br>The amount authorised by the bank. |
| p7 | 10 | **Card Type** - *Alpha*<br><br>The card type selected by the cardholder from the dropdown menu on the VCS page, i.e. ***MasterCard***, ***Visa***, ***Amex*** or ***Diners***. |
| p8 | 50 | **Description of Goods** - *Alphanumeric*<br><br>Description of goods from the incoming request |
| p9 | 255 | **Cardholder Email Address** - *Alphanumeric*<br><br>Cardholder email address if entered on the VCS payment page. |
| p10 | 2 | **Budget Period** - *Numeric*<br><br>Budget period entered by the cardholder on the VCS payment page, e.g. ***00*** is on straight. |
| p11 | 4 | **Expiry Date** - *Numeric*<br><br>Expiry date entered by the cardholder on the VCS payment page. The format is yymm. |
| | | |

| | | |
|---|---|---|
| p12 | 1 or 2 | **Bank Authorisation Response Code** - *Alphanumeric*<br><br>The authorisation response code received from the bank. For example, ***00*** is for an approved response (or 0 where Nedbank is the acquiring bank), and ***05*** is for a declined bank response, etc. |
| pam | 50 | **Personal Authentication Message** – *Alphanumeric*<br><br>The PAM is a security feature to confirm that the response received is actually from VCS. The merchant enters the PAM in Virtual Terminal and VCS returns that value as the PAM in the response. |
| m_1 to m_10 | 100 | **Merchant Parameters** – *Alphanumeric*<br><br>The merchant parameters are returned with all responses, exactly as they were presented in the original request. |
| CardHolderIpAddr | 15 | **IP address** - *Numeric plus dot*<br><br>The IP address of the browser used to enter the payment details. |
| MaskedCardNumber | 16 | **Masked Card Number** - *Numeric plus asterisk*<br><br>The card number as it was entered by the cardholder on the payment page, e.g. ***123456******1234***. |
| TransactionType | 13 | **Transaction Type** – *Alpha*<br><br>The possible transaction type values are ***Authorisation***, ***Settlement***, and ***Refund***, and correspond with the original request type.<br>For an authorisation request VCS will return "&TransactionType=Authorisation"<br>For a settlement request VCS will return "&TransactionType=Settlement"<br>For a refund request VCS will return "&TransactionType=Refund" |
| Hash | 32 | **MD5 Hash** - *Alphanumeric*<br><br>If hashing is activated VCS will return an MD5 hash of specific output parameters, and the shared secret (refer to hash response concatenation sequence). The hash can be either upper or lower case; it does not affect the hash itself. To compare a hash generated from the VCS response, convert both to the same case before comparing them. |

| | | |
|---|---|---|
| Uti | 36 | **Unique Transaction Id** - *Alphanumeric*<br><br>Required in South Africa |
| threeDsecureEnrolled | 1 | **3D Secure Enrolment Status** - *Alpha*<br><br>Response messages that are obtained include:<br>***Y*** means that the validation was successful and the issuer and cardholder are participating.<br>***N*** refers to a non-participating issuer or non-participating cardholder.<br>***U*** means that the acquirer was unable to validate due to an exemption, disconnect, no connection, an incorrect link, or to incorrect details provided. |
| threeDsecureEci | 2 | **3D Secure Electronic Commerce Indicator** - *Numeric*<br><br><u>MasterCard:</u><br>ECI ***01*** means that the cardholder is not enrolled.<br>ECI ***02*** means that the cardholder authentication was successfully completed.<br><u>Visa:</u><br>ECI ***05*** refers to a fully authenticated transaction. The cardholder is enrolled and the authentication process was followed.<br>ECI ***06*** means that the merchant is participating but the card was not enrolled.<br>ECI ***07*** is for unauthenticated transactions. The transaction liability is with the merchant. |
| threeDsecureXid | 16 | **3D Secure Transaction ID** - *Alphanumeric*<br><br>The authentication control server returns authentication data, including the transaction ID (XID) that's necessary to build a 3D secure authorisation request. |
| threeDsecureCavv | 200 | **Cardholder Authentication Verification Value** - *Alphanumeric*<br><br>The 3D secure authentication control server returns authentication data, including the cardholder authentication verification value (CAVV), that's necessary to build a 3D Secure authorisation request. |
| RetrievalReferenceNumber | 12 | **Retrieval Reference Number** - *Alphanumeric*<br><br>The retrieval reference number (RRN) is a unique identifier that can be used to uniquely identify a transaction. |

## 4. ON DEMAND OR TOKENIZED HOST TO HOST AUTHORISATION

Before using the on demand service, a token, or template, must have been created by one of the following methods. Either an authorisation request, using VCSPAY, with the recurring parameters set (the “Occur Frequency” set to “O”) must have been processed, and approved, so that the template is saved by the system. Or the Svc_VirtualRecur web service must have been called using the addCCTransaction method to add an “On Demand” template.

Either of these will cause the VCS system to save an “On Demand” token or template using the cardholder’s data and to store it into the VCS recurring transaction system, identified by the terminal Id and the first fifteen characters of the reference number.

When the merchant later presents an on demand authorisation request with the same terminal / user Id and reference number, the VCS system will retrieve the cardholder’s details, and use them for the new authorisation request. The reference number of the new request will be the first fifteen characters of the original reference followed by “-xxxxxxxxx” where xxxxxxxxx is a sequence number starting from 000000001. The VCS system will then return an approved or not-approved bank response.

### 4.1 ON DEMAND AUTHORISATION REQUEST EXAMPLE

The following code is used to request an on demand authorisation.
Create an HTML POST to the VCS 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 and URLEncoded XML Document.

#### 4.1.1 VBScript example

```
Dim xmlServerHttp
Dim xmlServerStatus
Dim XmlServerResponse

Set xmlServerHttp = Server.CreateObject("MsXml2.ServerXmlHTTP.6.0")

xmlServerHttp.open "POST","https://www.vcs.co.za/vvonline/ccxmldemand.asp",False
xmlServerHttp.setRequestHeader "Content-Type","application/x-www-form-urlencoded"
xmlServerHttp.send "xmlmessage=" & Server.URLEncode(xmlDocument)
‘ xmlDocument = the Xml Document contain the actual request
xmlServerStatus = xmlServerHttp.status

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

set xmlServerHttp = nothing

further processing of the xmlServerResponse ..
```

#### 4.1.2 Xml Document

```
<?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 | DESCRIPTION |
|---|---|---|
| UserId | 10 | **VCS Terminal ID** – *Alphanumeric*<br><br>Allocated by VCS. |
| Reference | 25 | **Reference Number or Token** – *Alphanumeric*<br><br>The reference number from the original authorization request. This reference must match a previously loaded token or template.<br>VCS only uses the first 15 characters of the original reference number when creating the token or template. VCS adds a "-" plus a nine digit left zero filled sequence number to the original reference number to make the reference unique per request. |
| Description | 50 | **Description of Goods** – *Alphanumeric* |
| Amount | 6.2 | **Transaction Amount** - N*umeric*<br><br>Specify the amount for the new on demand transaction. |
| m_1 to m_10 | 100 | **Merchant Parameters** - *Alphanumeric*<br><br>The m_ fields are optional merchant variables that echo. They can be set to anything and will be returned with the response. |

### 4.3 ON DEMAND AUTHORISATION RESPONSE EXAMPLE

```
Character Set UTF-8
<?xml version="1.0" ?>
        <DemandResponse>
                <UserId>XXXX</UserId>
                <Reference> abc123-yymmddhh</Reference>
                <Response>123456APPROVED</Response>
                <AdditionalResponseData />d
                <CardholderName>Name</CardholderName>
                <Amount>1.00</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>
        </DemandResponse>
```

### 4.4 ON DEMAND AUTHORISATION RESPONSE PARAMETER TABLE

| NAME | SIZE | DESCRIPTION |
|---|---|---|
| UserId | 10 | **VCS Terminal ID** – *Alphanumeric*<br><br>Allocated by VCS. |
| Reference | 25 | **Reference Number** – *Alphanumeric*<br><br>Reference number from the original authorisation request plus the "-xxxxxxxxx" that VCS added to the original reference number to make the on demand references unique, e.g. Inv00001dup-000000001 |
| Response | | **Authorisation Response** – *Alphanumeric*<br><br>The authorisation response returned by the bank.<br>For an approved transaction the first six characters contain the bank's alphanumeric authorisation number. From character seven |

| | | |
|---|---|---|
| | | expect the constant word APPROVED, left justified right space filled.<br>Not approved transactions contain the bank's reason for the declined authorisation request, e.g. not sufficient funds. |
| AdditionalResponseData | | The word **Duplicate** if a duplicate transaction reference number has been presented. VCS is merely returning the response from the first attempt. |
| CardholderName | 30 | **Cardholder Name** – *Alphanumeric*<br><br>Returning the cardholder name. |
| Amount | 6.2 | **Amount** - *Numeric and dot*<br><br>The amount of the authorisation request. |
| DescrOfGoods | 50 | **Description of Goods** – *Alphanumeric*<br><br>Returning the description of goods. |
| CardholderEmail | 255 | **Cardholder Email Address** – *Alphanumeric*<br><br>Returning the cardholder email address. |
| BudgetPeriod | 2 | **Budget Period** - N*umeric*<br><br>Returning the budget period. |
| ExpiryDate | 4 | **Expiry Date** - N*umeric*<br><br>Returning the expiry date. The format is yymm. |
| ResponseCode | 2 | **Authorisation Response Code** – *Alphanumeric*<br><br>Authorisation response code received from the bank. |
| MerchPam | 50 | **Personal Authentication Message** – *Alphanumeric*<br><br>The PAM is 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. |
| m_1 to m_10 | 100 | **Merchant Parameters** – *Alphanumeric*<br><br>Merchant parameter(s), m_1 to m_10, returned. |
| MaskedCardNumber | 16 | **Masked Card Number** - *Numeric plus asterisk*<br><br>Returning the masked card number, 123456******1234. |

## 4.5 THE RECURRING TEMPLATE ADMINISTRATION WEB SERVICE

The web service can be called using the API described at:
https://www.vcs.co.za/wscs/svc_virtualrecur.asmx

Username and password are the credentials required to access the system.
User Id and reference number are the unique identification of one particular template.
The following four parameters are always required.

| NAME | SIZE | DESCRIPTION |
|---|---|---|
| UserName | | The credentials required to make a call to the system, to modify a group of transactions. |
| Password | | For the above username. |
| UserId | 10 | The VCS Terminal ID allocated by VCS. |
| ReferenceNumber | 25 or 15 for recurring | With the UserId the ReferenceNumber uniquely identifies one transaction template. |

The web service has the following methods:

### 4.5.1 AddCCTransaction

Used for adding new templates to the system.

| NAME | SIZE | DESCRIPTION |
|---|---|---|
| CardNumber | 16 | Numeric |
| CardExpiryYy | 2 | Numeric. The year of the card expiry date. |
| CardExpiryMm | 2 | Numeric. The month of the card expiry date. |
| CVC | 3 | Numeric. The card validation code. |
| Amount | 6.2 | Numeric |
| CardHolderName | 20 | Alpha |
| CardHolderEmail | 255 | Alphanumeric |
| DescrOfGoods | 50 | Alphanumeric |
| StartDate | 8 | Date |
| EndDate | 8 | Date |
| OccurCount | 2 | Numeric |
| Frequency | 1 | Alphanumeric |
| MerchantVar1 | 100 | Alphanumeric |

### 4.5.2 UpdateCCTransaction

Used for making changes to the template information excluding the card and cardholder.

| NAME | SIZE | DESCRIPTION |
|---|---|---|
| Amount | 6.2 | Numeric |
| CardHolderName | 20 | Alpha |
| CardHolderEmail | 255 | Alphanumeric |
| DescrOfGoods | 50 | Alphanumeric |

| | | |
|---|---|---|
| StartDate | 8 | Date |
| EndDate | 8 | Date |
| OccurCount | 2 | Numeric |
| Frequency | 1 | Alphanumeric |
| MerchantVar1 | 100 | Alphanumeric |

**4.5.3 UpdateCCNumber**

Used for updating card information.

| NAME | SIZE | DESCRIPTION |
|---|---|---|
| CardNumber | | Numeric |
| CardExpiryYy | 16 | Numeric. Year of Card expiry. |
| CardExpiryMm | 2 | Numeric. Month of Card expiry. |
| CVC | 2 | Numeric. Card Validation Code. |
| CardHolderName | 3 | Alpha |

**4.5.4 DeleteCCTransaction**

Used for deleting templates.
Only user Id and reference number are required.

**4.5.5 SuspendCCTransaction**

Used for changing the status to suspended. No further transaction will process.
Only user Id and reference number are required.

**4.5.6 ActivateCCTransaction**

Used for changing the status of suspended templates back to Active status so that further transactions can process.
Only user Id and reference number are required.

**4.5.7 GetTransactionList**

Used for listing all the templates.
Only user Id is required.

**4.5.8 GetCCTransactionDetail**

Used for retrieving the detail for one individual transaction.
Only user Id and reference number are required.

# 5. REPORTING

## 5.1 DAILY REPORTS

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

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

**Outstanding Settlement Report** – a list of approved transactions, that VCS has not received settlement confirmation for. Settlement can be delayed at the bank by week-ends, public holidays or by the bank's risk management department's security checks.

**Settlement Report** – a list of approved transactions that VCS has received settlement confirmation for from the bank. The settlement report totals should match the banks (batch) payment that reflects on the merchant's bank statement. This report is for reconciliation purposes.

**Balance Report** – a summary of all the transactions presented from 00:00hr on the first day of a month until 23:59hr of the day before the date it is produced. It excludes transaction done since midnight the previous night. At the end of the month it will reset to zero BFWD for the new month.

## 5.2 REPORTING FORMAT

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

**FTP files** - VCS can create files, instead of email reports, and store these files in an FTP directory. These can then be collected when convenient. Please request the FTP output file specifications from support@vcs.co.za.

**Host to host settlement mark-up** – Overnight, every night except Sunday night, VCS receives settlement mark-up data from the bank. This data confirms the settlement of approved transactions. VCS can post the settlement parameters to the merchant's mark-up URL to provide confirmation of settlement.

## 5.3 HOST TO HOST SETTLEMENT MARK-UP REPORTING

To activate the host to host mark-up call-back function refer to the Merchant Settings section of this document.
The merchant must always return <CallbackResponse>Accepted</CallbackResponse> to VCS when VCS invokes the mark-up URL.

### 5.3.1 Example of host to host mark-up

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

This example shows the response when the Merchant setting's call-back response format has been set to Name Value Pairs.

### 5.3.2 Host to host settlement mark-up parameter table

| NAME | SIZE | DESCRIPTION |
|---|---|---|
| p1 | 10 | **VCS Terminal Id** - *Alphanumeric*<br><br>Allocated by VCS |
| p2 | 25 | **Unique Transaction Reference Number** - *Alphanumeric*<br><br>From the authorisation request, allocated by the merchant. |
| p6 | 6.2 | **Settlement Amount** – *Numeric*<br><br>For purchases the amount will not contain a sign indicator, e.g. &p6=123.45<br>For refunds the amount will contain a negative sign indicator, e.g. &p6=-123.45 |
| MarkupType | 6 | **Transaction Type** - *Alpha*<br><br>For authorisations the transaction type will be ***Debit***, e.g. &MarkupType=Debit<br>For refund settlements the transaction type will be ***Credit***, e.g. &MarkupType=Credit |

| | | |
|---|---|---|
| MarkupReference | 16 | **Mark-up Reference Number** - *Alphanumeric*<br><br>The mark-up reference number allocated by the bank. |
| MarkupDateTime | 19 | **Settlement Date and Time** - *Alphanumeric*<br><br>The date and time that the settlement was processed.<br>The format is ccyy/mm/dd hh:mm:ss (URL encoded). |
| pam | 50 | **Personal Authentication Message** – *Alphanumeric*<br><br>The PAM is a security feature to confirm that the response received is actually from VCS. The merchant enters the PAM in Virtual Terminal and VCS returns that value as the PAM in the response. |
| m_1 to m_10 | 100 | **Merchant Parameters** – *Alphanumeric*<br><br>The merchant parameters are returned with all responses, exactly as they were presented in the original request. |
| MaskedCardNumber | 16 | **Masked Card Number** - *Numeric plus asterisk*<br><br>The card number of the card that was debited or credited, e.g. 123456******1234. |
| Hash | 32 | **MD5 Hash** - *Alphanumeric*<br><br>If hashing is activated VCS will return an MD5 hash. |

## 6. MERCHANT SETTINGS

Go to https://www.vcs.co.za
Click Virtual Terminal
Enter the user login name and password
Click the **Merchant Administration** link

**1) Load response URLs and customize payment page:**

Select *3. VCS Interfacing (page1)* from the drop down
Enter merchant's approved and declined URLs
Select the Http method (POST or GET)
Save the settings

Click *Customized Payment Page >>* to access CSS for merchant's payment page
Click the item on the right that requires editing.
Select the option on the left.
Save the changes when editing has been completed.

**2) Load merchant PAM:**

Select *4. VCS Interfacing (page2)* from the drop down
Enter Merchant PAM.
The PAM is returned in the response parameters

**3) Activate callback settings:**

Select *6. Callback Settings* to activate the real-time authorisation call-back function and the daily settlement mark-up call-back

- To activate the call-back function set "Do Auth Callback" to "Yes"

Enter the call-back URLs
Select the protocol, method and format
Click Modify

- To activate the daily settlement mark-up call-back set the "Do Markup Callback" to Yes

Enter the mark-up URL
Select the protocol, method and format
Click Modify

## 7. TEST

New merchants loaded on the VCS system have access to the VCS Test platform.
In test mode VCS runs a response generator that provides simulated responses.

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.

Test Card Numbers:

Use any CVC number, e.g. 123, and any valid expiry date for the test card numbers.

Visa - 4242424242424242

MasterCard - 5454545454545454
MasterCard - 5221001010000024
MasterCard - 5221001010000032
MasterCard - 5221001010000040

Any valid credit card number can be submitted to the test platform during the test phase as the transactions are not sent to the banks for authorization, and no real money is involved.

## 8. ACTIVATION

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