



PayWeb

February 2012

Version 1.0
Revision 0.15

VERSION HISTORY.....	3
INTRODUCTION	3
BENEFITS TO PAYWEB	3
A QUICK SAMPLE.....	4
PAYGATE ACCOUNT SETUP OPTIONS – PER PAYGATEID	4
<i>Password & Card Types Accepted</i>	<i>4</i>
<i>Auto-Settle : Default is ON.....</i>	<i>4</i>
<i>Process Unauthenticated Transactions : Default is OFF.....</i>	<i>4</i>
<i>PayProtector : Default is Not Activated.....</i>	<i>4</i>
SETUP OPTIONS WHEN MORE THAN ONE PAYMENT METHOD IS ACTIVATED	5
PROCESS FLOW.....	5
THE ‘LANDING’ PAGES.....	6
PAYMENT MENU PAGE	6
PAYMENT PAGE	7
HOW TO GET IT WORKING – REQUEST AND RESPONSE	8
THE REQUEST	8
CHECKSUM EXAMPLE	9
REQUEST EXAMPLES	9
THE RESPONSE.....	9
RESPONSE EXAMPLE	11
MISCELLANEOUS INFORMATION	11
SECURITY.....	11
CUSTOMISING THE PAYMENT PAGE	12
TESTING.....	13
MASTERCARD SECURECODE & VERIFIED BY VISA.....	14
<i>A typical credit card authorisation flow including PayProtector and 3D.....</i>	<i>15</i>
FREQUENTLY ASKED QUESTIONS	16
<i>How do I know the transaction is approved?</i>	<i>16</i>
<i>I'm using VBScript / JScript in ASP and I can't find an MD5 function?.....</i>	<i>16</i>
<i>Can I do the authorisation and the settlement separately?</i>	<i>16</i>
<i>What response is returned if the customer clicks the ‘Cancel’ button on the PayWeb payment page?</i>	<i>16</i>
<i>How will I know that I the transaction was authenticated and I have charge back protection?</i>	<i>16</i>
<i>The transaction was authenticated and declined; how can this be?</i>	<i>16</i>
<i>Is it possible to not make use of MasterCard SecureCode / Verified by Visa?</i>	<i>16</i>
APPENDIX A : CODES & DESCRIPTIONS	17
RESULT CODES	17
TRANSACTION STATUS.....	18
MASTERCARD SECURECODE / VERIFIED BY VISA AUTHENTICATION INDICATOR	18
COUNTRY AND CURRENCY CODES	18

Version History

Version	Date	Comment
1.1	August 2005	Document created
1.2	August 2005	Wording changes
1.3	April 2006	Added new Result Codes
1.4	April 2006	MasterCard SecureCode / Verified-by-Visa added; Risk Indicator added in response
1.5	June 2006	Wording changes
1.6	July 2006	Risk Indicator changed from optional to required
1.7	May 2007	Added new test credit cards; fixed request examples
1.8	September 2007	Specified field length for the Reference
1.9	March 2008	Added new Result Codes; updated test credit cards
1.10	August 2008	Added FNB Cell Pay Point and Mobux payment methods as well as test details.
1.11	June 2009	Added Ukash as a payment method; also added Ukash test vouchers and cards.
1.15	February 2012	Added payD and SiD

Introduction

PayWeb is a secure PCI compliant payment system hosted by PayGate. A single integration to PayWeb gives you access to multiple payment methods.

PayGate is continually adding to the list of available payment methods. We currently support the following :-

- MasterCard / Visa / AMEX / Diners card processing (with or without 3D Secure)
- Debit card (via the payD (AMT) method). Currently only applies to South African card holders.
- Ukash voucher
- PaySum1 – local bank transfers for forex payments.
- SiD EFT – Automated Electronic Funds Transfer using the clients internet banking
- FNB Cell Pay Point – a mobile payment solution for registered FNB mobile banking clients

Benefits to PayWeb

- The setup process is relatively simple and can be easily integrated into existing web sites.
- The merchant doesn't require a SSL certificate to capture the credit card details as PayGate provides this.
- PayWeb can be customised to suit the look & feel of your web site.
- Access to multiple payment methods from a single integration.
- MasterCard SecureCode and Verified by Visa payer authentication is built in to minimize the risk of charge backs for credit card transactions.
- PayGate's PayProtector fraud and risk system can be activated for PayWeb.
- PayWeb is PCI compliant.

A Quick Sample

- Copy & paste the code block below into a new text document (NotePad).
- Save the new text document as 'PayWeb.htm' into the 'My Documents' folder.
- Double-click on the new file created; it will open a Browser window displaying a 'Submit' button.
- Click the 'Submit' button; you will be directed to the PayWeb processing page.

Note: This sample is only intended to demonstrate how to connect to PayWeb; it does not demonstrate how to read the results of a transaction. Please see SAMPLES for links to complete examples.

```
<html>
<head>
  <title>PayGate::PayWebv2 Sample</title>
</head>
<body>
  <form action="https://www.paygate.co.za/paywebv2/process.trans" method="POST" >
    <input type="hidden" name="PAYGATE_ID" value="10011013800">
    <input type="hidden" name="REFERENCE" value="Customer1">
    <input type="hidden" name="AMOUNT" value="3299">
    <input type="hidden" name="CURRENCY" value="ZAR">
    <input type="hidden" name="RETURN_URL" value="http://localhost">
    <input type="hidden" name="TRANSACTION_DATE" value="2012-01-30 18:30:00">
    <input type="hidden" name="CHECKSUM" value=" 31d1244f08a62f0551e9263c4835ba88">
    <input type="submit" value="Submit">
  </form>
</body>
</html>
```

PayGate account setup options – per PayGateID

The following parameters are configured for each PayGate account (ie. per PayGateID). These are agreed and pre-set when your account with PayGate is configured by our support team.

Password & Card Types Accepted

Merchants are given access to the PayWeb configuration page (via the PayGate BackOffice) where they set the following options:

- The password / encryption key used in the checksum calculation.
- Choose which credit card brands to accept. MasterCard and Visa are enabled by default.

Auto-Settle : Default is ON

Applies to : card processing.

With this option enabled, you do not need to send a Settlement transaction for an approved Authorisation. As soon as the bank approves the Authorisation, PayGate immediately and automatically creates the Settlement transaction on your behalf. This option is enabled by default

Process Unauthenticated Transactions : Default is OFF

Applies to : card processing with a 3D Secure integration.

Any MasterCard or Visa transaction that is not authenticated through Verified-by-Visa / MasterCard SecureCode is declined and not sent to the bank for authorisation. Enabling this option allows the merchant to send unauthenticated transactions to the bank for authorisation. The option is disabled by default and we discourage merchants from enabling this option, as they will not receive chargeback protection on fraudulent transactions.

PayProtector : Default is Not Activated

Applies to : card processing.

PayProtector is PayGate's fraud and risk system, designed to help the merchant minimise the risk of loss from fraudulent transactions. Fraud has become a serious problem and often adds significant costs for internet merchants. PayProtector scrutinises transactions from a number of angles combining internal, local and international information to identify, report on, and / or block fraudulent transactions.

Please contact support@paygate.co.za if you would like more information on PayProtector.

Setup options when more than one payment method is activated

PayGate allows merchants to have multiple PayGateID's.

Each PayGateID has access to the PayGate back office and all transactions processed by PayGate using a particular PayGateID are visible in the back office. Reports can be viewed in the back office or downloaded into MS Excel (or similar) applications for offline reporting.

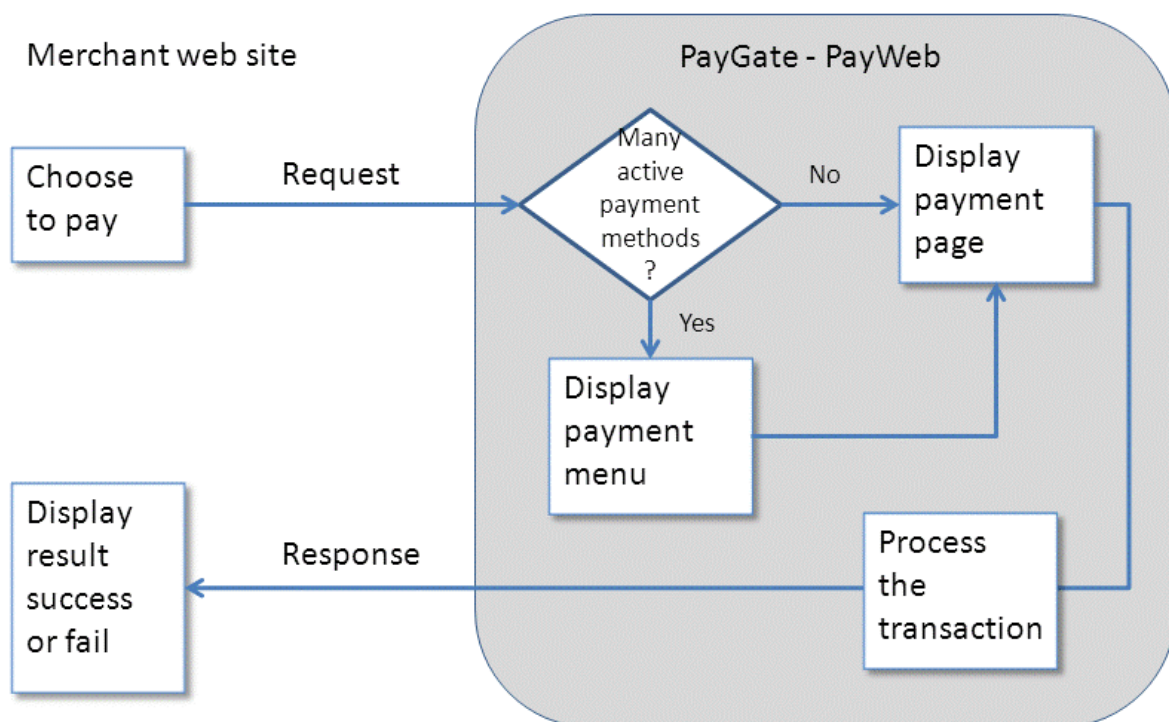
A merchant with multiple payment methods can choose to either :-

- a) have multiple payment methods all activated on a single PayGateID or
- b) to have multiple PayGateID's with a single payment method active per PayGateID.

If option a) is chosen, then PayWeb will display a menu of payment options to the client. The client will choose how (s)he wants to pay and select the relevant menu option.

If option b) is chosen, then the client will be taken directly to the relevant payment page.

Process flow




The 'landing' pages

Payment menu page

The menu page is only displayed to the client if more than one payment method is activated on the PayGateID. Only active payment methods are displayed. This page is customisable and an iFrame can be used to maintain the look and feel of the merchant system as far as possible. ([Refer to Customising the Payment Page](#)).

Example of a (not customised) payment menu page

Merchant	PayGate Test
VAT Registration #	123456789012345
Reference	TEST REFERENCE
Transaction Date	Tue, 07 Feb 2012 17:47:08 +0200
Amount	R 30.99 (ZAR)




Please select a payment type

Credit Card

Debit Card with PIN

FNB Cell Pay Point

Ukash


2012-02-07

E-Mail Address (for payment confirmation)	support@paygate.co.za
---	-----------------------

Welcome to the PayWebv2 test page. This message can be customised.

<- Cancel


Payment page

The payment page will vary depending on the payment method.





This page is customisable and an iFrame can be used to maintain the look and feel of the merchant system as far as possible. ([Refer to Customising the Payment Page](#)).

Example of a (not customised) credit card payment page

Merchant	PayGate Test
VAT Registration #	123456789012345
Reference	TEST REFERENCE
Transaction Date	Tue, 07 Feb 2012 17:47:08 +0200
Amount	R 30.99 (ZAR)



Cards Accepted



Card Holder

Card Number

Expiry Date

Jan 2012


CVV Digits
(3/4 digits on back of card)

[what's this?](#)

Budget Period
(South African Card Holder Only)

0 months

Change Payment Type



E-Mail Address
(for payment confirmation)

support@paygate.co.za

Welcome to the PayWebv2 test page. This message can be customised.

<- Cancel

Pay Now ->

How to get it working – Request and Response

There are 2 steps when connecting a web site to PayWeb. The 1st step is sending the **Request** to PayWeb to show the payment screen (or payment menu if applicable) to the customer. The 2nd step involves collecting the results (**Response**) of the transaction from PayWeb.

The Request

All information sent to PayWeb must be in hidden form fields (as in the [Quick Sample](#) above), which are posted to the PayWeb web page.

The HTML form element should resemble:

```
<form action="https://www.paygate.co.za/PayWebv2/process.trans" method="POST" >
```

The hidden fields are described below:

Field	Type	Required
PAYGATE_ID Your PayGateID – assigned by PayGate. e.g. <code><input type="hidden" name="PAYGATE_ID" value="10011013800"></code>	Number(11)	Yes
REFERENCE This is your reference number for use by your internal systems. e.g. <code><input type="hidden" name="REFERENCE" value="Customer1"></code>	Varchar(80)	Yes
AMOUNT Transaction amount in cents. e.g. 32.95 is specified as 3295 <code><input type="hidden" name="AMOUNT" value="3299"></code>	Number(11)	Yes
CURRENCY Currency code of the currency the customer is paying in. Refer to appendix A for valid currency codes e.g. <code><input type="hidden" name="CURRENCY" value="ZAR"></code>	Char(3)	Yes
RETURN_URL Once the transaction is completed, PayWeb will return the customer to a page on your web site. The page the customer must see is specified in this field. e.g. <code><input type="hidden" name="RETURN_URL" value="http://www.mywebsite.com/thanks.php"></code>	Varchar(255)	Yes
TRANSACTION_DATE This is the date that the transaction was initiated on your website or system. The transaction date must be specified in 'Coordinated Universal Time' (UTC) and formatted as 'YYYY-MM-DD HH:MM:SS'. e.g. <code><input type="hidden" name="TRANSACTION_DATE" value="2012-01-30 18:30:00"></code>	Varchar(19)	Yes
EMAIL The email address of your customer is optional; if it is not supplied, PayWeb will prompt the customer for their email address when entering their payment details. If the transaction is approved, PayWeb will email a payment confirmation to this email address. If the email address is supplied, it must be included in the CHECKSUM calculation described below. e.g. <code><input type="hidden" name="EMAIL" value="customer@mywebsite.com"></code>	Varchar(255)	No
CHECKSUM This field contains a calculated MD5 hash based on the values of the above-mentioned fields and a key . The key is only known by the merchant and PayGate (via the PayGate BackOffice) and should not be displayed on the merchant's web site. PayWeb does the same calculation when the request is received to ensure that the data has not been tampered with. Refer to the section on Security below for more detail regarding the MD5 hash. e.g. refer to the ' CHECKSUM example' below	Varchar(32)	Yes

CHECKSUM example

All fields are separated with a pipe (the | character) to form the source of the MD5 hash (optional fields in *italics*):

PAYGATE_ID|REFERENCE|AMOUNT|CURRENCY|RETURN_URL|TRANSACTION_DATE|EMAIL|KEY

Assuming the **KEY** is 'secret', the following scenarios are possible:

1. Without the **EMAIL** field, the checksum source would translate to:

10011013800|Customer1|3299|ZAR|http://www.mywebsite.com/thanks.php|2012-01-30 18:30:00|secret

The MD5 hash value for this transaction would be: 928ad0f73064d137c4af14457954f8a1

<input type="hidden" name="CHECKSUM" value="928ad0f73064d137c4af14457954f8a1">

2. With the **EMAIL** field, the checksum source would translate to:

10011013800|Customer1|3299|ZAR|http://www.mywebsite.com/thanks.php|2012-01-30 18:30:00|customer@mywebsite.com|secret

The MD5 hash value for this transaction would be: 928ad0f73064d137c4af14457954f8a1

<input type="hidden" name="CHECKSUM" value="928ad0f73064d137c4af14457954f8a1">

Request Examples

These examples assume the Encryption Key '**secret**' was used as part of the **CHECKSUM** calculation.

Without the EMAIL field:

```
<form action="https://www.paygate.co.za/paywebv2/process.trans" method="POST" >
  <input type="hidden" name="PAYGATE_ID" value="10011013800">
  <input type="hidden" name="REFERENCE" value="Customer1">
  <input type="hidden" name="AMOUNT" value="3299">
  <input type="hidden" name="CURRENCY" value="ZAR">
  <input type="hidden" name="RETURN_URL" value="http://www.mywebsite.com/thanks.php">
  <input type="hidden" name="TRANSACTION_DATE" value="2012-01-30 18:30:00">
  <input type="hidden" name="CHECKSUM" value="928ad0f73064d137c4af14457954f8a1">
</form>
```

With the EMAIL field:

```
<form action="https://www.paygate.co.za/paywebv2/process.trans" method="POST" >
  <input type="hidden" name="PAYGATE_ID" value="10011013800">
  <input type="hidden" name="REFERENCE" value="Customer1">
  <input type="hidden" name="AMOUNT" value="3299">
  <input type="hidden" name="CURRENCY" value="ZAR">
  <input type="hidden" name="RETURN_URL" value="http://www.mywebsite.com/thanks.php">
  <input type="hidden" name="TRANSACTION_DATE" value="2012-01-30 18:30:00">
  <input type="hidden" name="EMAIL" value="customer@mywebsite.com">
  <input type="hidden" name="CHECKSUM" value="928ad0f73064d137c4af14457954f8a1">
</form>
```

The Response

Once PayWeb has completed the transaction, it returns the customer to the merchant's web site. The results of the transaction are posted in hidden fields similar to the Request.

The Response hidden fields are detailed below:

Field	Type	Required
PAYGATE_ID This should be the same PayGate ID that was passed in the request; if it is not, then the data has been altered. e.g. <input type="hidden" name="PAYGATE_ID" value="10011013800">	Number(11)	Yes
REFERENCE This should be the same reference that was passed in the request; if it is not, then the data has been altered. e.g. <input type="hidden" name="REFERENCE" value="Customer1">	Varchar(80)	Yes

TRANSACTION_STATUS The final status of the transaction. Refer to the Transaction Status table for a list of possible values. e.g. <input type="hidden" name="TRANSACTION_STATUS" value="1">	Number(1)	Yes
RESULT_CODE This field contains a code indicating the result of the transaction. Refer to the Result Code table for a complete list. The description corresponding to this code is in the RESULT_DESC field. e.g. <input type="hidden" name="RESULT_CODE" value="990017">	Number(11)	Yes
AUTH_CODE If the bank approves the credit card transaction, then the authorisation code will be placed in this field. This is the merchants' guarantee that the funds are available on the customer's credit card. For non-card payment methods this field is populated with "999999". e.g. <input type="hidden" name="AUTH_CODE" value="015867">	Varchar(10)	Yes
AMOUNT This should be the same amount that was passed in the request. If it is not, then the data has been altered. e.g. <input type="hidden" name="AMOUNT" value="3299">	Number(11)	Yes
RESULT_DESC This field contains a description for the result of the transaction. Refer to the Result Code table for a complete list. The numeric code corresponding to this description is in the RESULT_CODE field. e.g. <input type="hidden" name="RESULT_DESC" value="Auth Done">	Varchar(80)	Yes
TRANSACTION_ID This field contains the PayGate unique reference number for the transaction. e.g. <input type="hidden" name="TRANSACTION_ID" value="25975624">	Number(11)	Yes
RISK_INDICATOR This is a 2-character field containing a risk indicator for this transaction. The first character describes the Verified-by-Visa / MasterCard SecureCode authentication; refer to the Authentication Indicator table for the possible values. The second character is for future use and will be set to 'X'. Please refer to the MasterCard SecureCode & Verified by Visa section for more info. e.g. <input type="hidden" name="RISK_INDICATOR" value="NX">	Char(2)	Yes
CHECKSUM The MD5 hash calculation of all the response fields including the key known only to the merchant and PayGate. You should do the same calculation when you receive the response to ensure that the data has not been tampered with. Refer to the section on Security below for more detail regarding the MD5 hash. All fields are separated with a pipe (the character) to form the source of the MD5 hash: PAYGATE_ID REFERENCE TRANSACTION_STATUS RESULT_CODE AUTH_CODE AMOUNT RESULT_DESC TRANSACTION_ID RISK_INDICATOR KEY Assuming the KEY is 'secret', the checksum source would translate to: 10011013800 Customer1 1 990017 015867 3299 Auth Done 5975624 NX secret The MD5 hash value for this transaction would be: a36bf8f89b7b4b26940eef45907be761 e.g. <input type="hidden" name="CHECKSUM" value="a36bf8f89b7b4b26940eef45907be761">	Varchar(32)	Yes

Response Example

This example assumes the Encryption Key '**secret**' was used as part of the **CHECKSUM** calculation.

```
<html>
<head>
  <title>PayGate::PayWebv2 Response Sample</title>
</head>
<body>
  <form action="http://www.mywebsite.com/thanks.php" method="POST" >
    <input type="hidden" name="PAYGATE_ID" value="10011013800">
    <input type="hidden" name="REFERENCE" value="Customer1">
    <input type="hidden" name="TRANSACTION_STATUS" value="1">
    <input type="hidden" name="RESULT_CODE" value="990017">
    <input type="hidden" name="AUTH_CODE" value="015867">
    <input type="hidden" name="AMOUNT" value="3299">
    <input type="hidden" name="RESULT_DESC" value="Auth Done">
    <input type="hidden" name="TRANSACTION_ID" value="5975624">
    <input type="hidden" name="RISK_INDICATOR" value="NX">
    <input type="hidden" name="CHECKSUM" value="a36bf8f89b7b4b26940eef45907be761">
  </form>
</body>
</html>
```

Miscellaneous Information

Security

Security is enhanced by making use of an MD5 checksum value that is passed in both the request to PayWeb and the response from PayWeb.

The checksum for the PayWeb **Request** is calculated by concatenating the fields (PAYGATE_ID, REFERENCE, AMOUNT, CURRENCY, RETURN_URL, TRANSACTION_DATE, EMAIL(optional)).

A password / encryption key is appended and the resulting string is passed through an MD5 hash algorithm to produce the checksum. When PayGate receives the PayWeb request, the same checksum calculation is performed. If the PayGate checksum does not match the checksum specified in the request, the transaction is rejected.

The checksum for the PayWeb **Response** is calculated by concatenating the fields (PAYGATE_ID, REFERENCE, TRANSACTION_STATUS, RESULT_CODE, AUTH_CODE, AMOUNT, RESULT_DESC, TRANSACTION_ID, RISK_INDICATOR).

The same password / encryption key used in the request is appended and the resulting string is passed through an MD5 hash algorithm to produce the checksum. **The merchant must do the checksum calculation when the response is received. If the calculated checksum does not match the PayGate checksum in the response, the results should be rejected.**

MD5 is a one-way hashing algorithm. Simply stated, input of any length supplied to the function produces a fixed length (in this case 32 characters) output so that the original input is not recognisable. It is impossible to reverse; i.e. giving the function the result will not give you the original source. Most programming languages support the MD5 function; if not native support then by a module or extension. You can find more information on MD5 implementation in various programming languages at the website:

<http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html>.

The Encryption Key used in the checksum calculation should only be known by the merchants' website and PayGate. It should not be displayed on any web page i.e. a customer should never be able to see it. PayGate allows for the Encryption Key to be a maximum of 32 alphanumeric characters. The longer and more complex the key is, the harder it is for a malicious user to guess it.

Customising the Payment Page

Merchants are given access to the PayWeb configuration page (via the PayGate BackOffice) where they are able to control the following 'look & feel' components of the PayWeb payment page:

- Background colours and font styles, colours & sizes
- Ability to upload & position a company logo
- Choose whether to allow budget transactions (applies to South Africa only).
- Choose which credit card brands to accept.
- A static message displayed to the customer.

The configuration page is also used to set the password / encryption key used in the checksum calculation.

The default test account does not allow any customisation. All options are enabled and there is no logo. If you would like us to create a unique test account which you can customise, then please go to the PayWeb v2 developer site: https://www.paygate.co.za/develop/paywebv2_login.php and click the 'apply for a test account' link. You will be provided with a Test PayGate ID that can be customised. Once your live PayGate account has been created, customisation made on the test account can be applied to your live account.

Testing

The default test PayGate ID is **10011013800**; all requests using this PayGate ID are processed to our test server. Please refer to the table below when testing to simulate predictable results:

Card Brand	Card Number	Risk Indicator
Approved Transactions. RESULT_CODE = 990017; TRANSACTION_STATUS = 1.		
Visa	4000000000000002	Authenticated (AX) *
MasterCard	5200000000000015	Authenticated (AX)
American Express	378282246310005	Not Authenticated (NX)
FNB Cell Pay Point	N/A; enter MR PASS in Account Holder field.	Authenticated (AX)
Ukash Voucher (with new voucher issued as change)	9999991500000000012	Authenticated (AX)
Ukash Voucher (with no change voucher issued)	9999991500000000020	Authenticated (AX)
Ukash Card	9826160000000005	Authenticated (AX)
payD / AMT / MobileMoney (Mobile phone is linked to a card)	0839998887	Authenticated (AX)
payD / AMT / MobileMoney (Mobile phone is <u>not</u> linked to a card)	0821112224 Then link this card 503615000000000018	Authenticated (AX)
payD / AMT / MobileMoney (Mobile phone is <u>not</u> linked to a card and expiry date is required)	0821112224 Then link this card 5120550000000016	Authenticated (AX)
Insufficient Funds Transactions. RESULT_CODE = 900003; TRANSACTION_STATUS = 2.		
MasterCard	5200000000000023	Not Authenticated (NX) *
Visa	4000000000000028	Not Authenticated (NX)
American Express	371449635398431	Not Authenticated (NX)
Declined Transactions. RESULT_CODE = 900007; TRANSACTION_STATUS = 2.		
Visa	4000000000000036	Authenticated (AX) *
MasterCard	5200000000000049	Authenticated (AX) *
Diners Club	30569309025904	Not Applicable (XX)
FNB Cell Pay Point	N/A; enter MR FAIL in Account Holder field.	Not Applicable (XX)
Ukash Voucher	9999991500000000038	Not Applicable (XX)
Ukash Card	9826160000000013	Not Applicable (XX)
payD / AMT / MobileMoney	0832544555 or any other number	Not Applicable (XX)
Invalid Card Number. RESULT_CODE = 900004; TRANSACTION_STATUS = 2.		
For credit card payment method - all other card numbers		Not Applicable (XX)
Unprocessed Transactions. RESULT_CODE = 990022; TRANSACTION_STATUS = 0.		
MasterCard	5200000000000064	Not Applicable (XX)
<i>Expiry Date must be in the future; Card Holder & CVV or Ukash PIN can be made up.</i>		

* = Using these card numbers will allow you to test the MasterCard SecureCode / Verified-by-Visa authentication process.

MasterCard SecureCode & Verified by Visa

What is Secure Code and Verified by Visa?

Secure Code and Verified by Visa is a MasterCard and Visa initiative to reduce online credit card transaction fraud. (It applies to Master and Visa cards only).

The Visa implementation is referred to as Verified by Visa or V-by-V.

The MasterCard implementation is referred to as MasterCard Secure Code.

How does Secure Code and Verified by Visa benefit the merchant?

It significantly reduces the risk of fraudulent transactions, and moves the risk of certain charge backs from the merchant to the card holder or the Issuing Bank.

(Note – there are instances where the charge back risk remains with the merchant – this is detailed in the flowchart below).

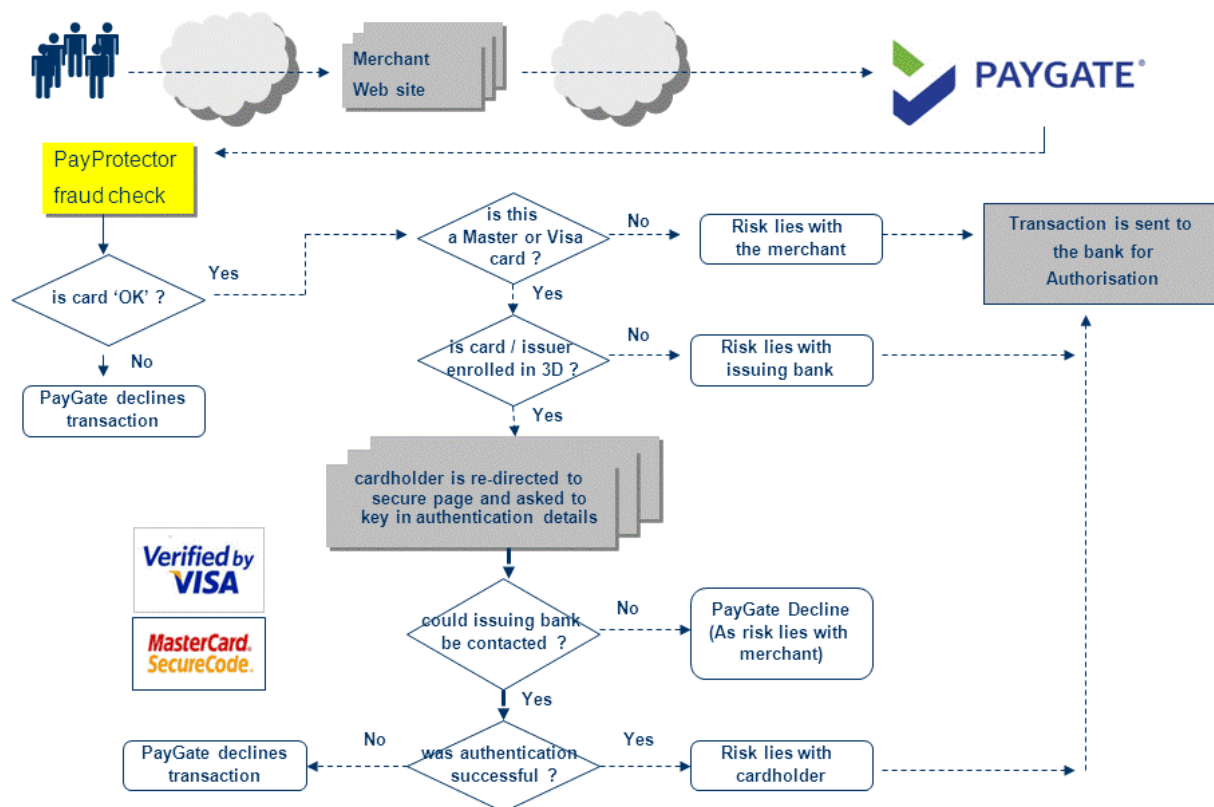
How Does Secure Code and Verified by Visa work?

When a purchase is made online, the cardholder will be re-directed from the secure PayGate payment page, to the issuing bank's (cardholder's bank) Secure Code and Verified by Visa authentication page. Here the cardholder will be required to key in his/her authentication details (e.g. secret PIN code). The Issuing Bank validates this code and returns an 'OK' or 'not OK' response to PayGate. If PayGate receives an 'OK' response then we pass the transaction on to the Acquiring Bank for Authorisation. If the response is 'not OK' then the transaction is 'Declined' up front by PayGate.

It should however be noted that not all Issuing Banks will force their cardholders to register for this service. Where this is the case, a re-direct will still take place to the issuing bank's website but in this case the transaction will not be authenticated. The message code returned, will however indicate that you as a merchant attempted to authenticate the transaction and that the issuing bank is not registered for the service. The transaction will be processed as a Secure Code and Verified by Visa transaction i.e. the risk will be passed to the issuing bank.

What about the other cards (AMEX, Diners etc)?

These cards are not authenticated via the Secure Code and Verified by Visa process. At this time transaction risk for purchases made with cards other than Master and Visa, will remain with the merchant.

A typical credit card authorisation flow including PayProtector and 3D

Frequently Asked Questions

How do I know the transaction is approved?

You can check up to 3 fields in the response depending on how thorough you want to be. At a minimum, you should check the TRANSACTION_STATUS field: it will contain the value "1". If you want to check further, the RESULT_CODE field should contain the value "990017" and the AUTH_CODE field should not be blank.

I'm using VBScript / JScript in ASP and I can't find an MD5 function?

Please refer to the site: <http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html> (or search on Google). It has links to developers that have already written the MD5 function in VBScript / Jscript that can be included on your site. Alternatively, download the PayWebv2 ASP sample from the PayGate site; the sample code contains a VBScript MD5 function.

Can I do the authorisation and the settlement separately?

Yes, PayGate has an 'Auto-Settle' configuration setting that is enabled by default for all merchants. This means that PayGate automatically creates the settlement transaction when a PayWeb request is approved. If you would prefer to only authorise the transaction when the customer enters their card details (i.e. no funds are transferred), please send an email to support@paygate.co.za to request that the 'Auto-Settle' feature be disabled. With the 'Auto-Settle' feature disabled, the merchant will have to login to the PayGate BackOffice and effect the settlement manually.

What response is returned if the customer clicks the 'Cancel' button on the PayWeb payment page?

- The TRANSACTION_STATUS field will contain "0".
- The RESULT_CODE field will contain "990028".
- The TRANSACTION_ID field will be blank.

How will I know that I the transaction was authenticated and I have charge back protection?

When your website receives the transaction results from PayGate, it should check the first character of the RISK_INDICATOR field. If the first character is 'A' then your customer has been authenticated and cannot initiate a charge back. If the first character is 'N' then the transaction has been declined or approved but not authenticated; you should take further steps to ensure that you are dealing with the legitimate card holder.

The transaction was authenticated and declined; how can this be?

PayGate attempts to authenticate the cardholder before sending the transaction to the bank for authorisation. Therefore even if the cardholder is authenticated through MasterCard SecureCode or Verified-by-Visa, the bank could still decline the transaction due to insufficient funds etc.

Is it possible to not make use of MasterCard SecureCode / Verified by Visa?

It is; but not recommended, as you will not receive any charge back protection. If you prefer not to make use of MasterCard SecureCode / Verified-by-Visa, please contact support@paygate.co.za.

Appendix A : Codes & Descriptions

Result Codes

Code	Description	Comment
Transaction Processing Errors – These RESULT_CODES are returned if the transaction cannot be authorised or successfully processed for any reason. The TRANSACTION_STATUS will be 2 .		
900001	Call for Approval	
900002	Card Expired	
900003	Insufficient Funds	
900004	Invalid Card Number	
900005	Bank Interface Timeout	Indicates a communications failure between the banks systems.
900006	Invalid Card	
900007	Declined	
900009	Lost Card	
900010	Invalid Card Length	
900011	Suspected Fraud	
900012	Card Reported As Stolen	
900013	Restricted Card	
900014	Excessive Card Usage	
900015	Card Blacklisted	
900207	Declined; authentication failed	Indicates the cardholder did not enter their MasterCard SecureCode / Verified by Visa password correctly.
900220	Incorrect PIN	
990020	Auth Declined	
991001	Invalid expiry date	
991002	Invalid Amount	
Transaction Successful – Indicates the transaction was approved. TRANSACTION_STATUS will be 1 .		
990017	Auth Done	
Communication Errors – These RESULT_CODES are returned if the transaction cannot be completed due to an unexpected error. TRANSACTION_STATUS will be 0 .		
900205	Unexpected authentication result (phase 1)	
900206	Unexpected authentication result (phase 1)	
990001	Could not insert into Database	
990022	Bank not available	
990029	Transaction Not Completed	
990053	Error processing transaction	
Miscellaneous - Unless otherwise noted, the TRANSACTION_STATUS will be 0 .		
900209	Transaction verification failed (phase 2)	Indicates the verification data returned from MasterCard SecureCode / Verified-by-Visa has been altered.
900210	Authentication complete; transaction must be restarted	Indicates that the MasterCard SecureCode / Verified-by-Visa transaction has already been completed. Most likely caused by a customer clicking the refresh button.
990024	Duplicate Transaction Detected. Please check before submitting	
990028	Transaction cancelled	Customer clicks the 'Cancel' button on the payment page.

Transaction Status

Transaction Code	Description
0	Not Done
1	Approved
2	Declined

MasterCard SecureCode / Verified by Visa Authentication Indicator

Code	Description	Comment
N	Not Authenticated	Authentication was attempted but NOT successful. Merchant does NOT receive charge back protection for this transaction.
A	Authenticated	Authentication was attempted and was successful. Merchant does receive charge back protection for this transaction.
X	Not Applicable	Authentication processing NOT enabled on PayGate account or unexpected error in authentication process. Merchant does NOT receive charge back protection for this transaction.

Country and Currency codes

Country	Country Code	Currency	Currency Code
Afghanistan	AFG	Afghani	AFA
Albania	ALB	Lek	ALL
Algeria	DZA	Algerian Dinar	DZD
American Samoa	ASM	U.S. Dollar	USD
Andorra	AND	Euro	EUR
Angola	AGO	Kwanza	AOA
Anguilla	AIA	E. Caribbean Dollar	XCD
Antarctica	ATA	Norwegian Krone	NOK
Antigua and Barbuda	ATG	E. Caribbean Dollar	XCD
Argentina	ARG	Argentine Peso	ARS
Armenia	ARM	Armenian Dram	AMD
Aruba	ABW	Aruban Guilder	AWG
Australia	AUS	Australian Dollar	AUD
Austria	AUT	Euro	EUR
Azerbaijan	AZE	Azerbaijan Manat	AZM
Bahamas	BHS	Bahamian Dollar	BSD
Bahrain	BHR	Bahraini Dinar	BHD
Bangladesh	BGD	Taka	BDT
Barbados	BRB	Barbados Dollar	BBD
Belarus	BLR	Belarussian Ruble	BYR
Belgium	BEL	Euro	EUR
Belize	BLZ	Belize Dollar	BZD
Benin	BEN	CFA Franc BCEAO	XOF
Bermuda	BMU	Bermudian Dollar	BMD
Bhutan	BTN	Indian Rupee	INR
Bolivia	BOL	Boliviano	BOB
Bosnia and Herzegovina	BIH	Bosnian Convertible Mark	BAM
Botswana	BWA	Pula	BWP
Bouvet Is.	BVT	Norwegian Krone	NOK
Brazil	BRA	Brazilian Real	BRL
British Indian Ocean Territory	IOT	U.S. Dollar	USD

British Virgin Is.	VGB	U.S. Dollar	USD
Brunei Darussalam	BRN	Brunei Dollar	BND
Bulgaria	BGR	Bulgarian Lev	BGN
Burkina Faso	BFA	CFA Franc BCEAO	XOF
Burundi	BDI	Burundi Franc	BIF
Cambodia	KHM	Riel	KHR
Cameroon United Republic of	CMR	CFA Franc BEAC	XAF
Canada	CAN	Canadian Dollar	CAD
Cape Verde Is.	CPV	Cape Verde Escudo	CVE
Cayman Is.	CYM	Cayman Is. Dollar	KYD
Central African Republic	CAF	CFA Franc BEAC	XAF
Chad	TCO	CFA Franc BEAC	XAF
Chile	CHL	Chilean Peso	CLP
China	CHN	Yuan Renminbi	CNY
Christmas Is.	CXR	Australian Dollar	AUD
Cocos (Keeling) Is.	CCK	Australian Dollar	AUD
Colombia	COL	Colombian Peso	COP
Comoros	COM	Comoro Franc	KMF
Congo	COG	CFA Franc BEAC	XAF
Cook Is.	COK	New Zealand Dollar	NZD
Costa Rica	CRI	Costa Rican Colon	CRC
Côte d'Ivoire (Ivory Coast)	CIV	CFA Franc BCEAO	XOF
Croatia	HRV	Croatian Kuna	HRK
Cuba	CUB	Cuban Peso	CUP
Cyprus	CYP	Cyprus Pound	CYP
Czech Republic	CZE	Czech Koruna	CZK
Democratic Republic of the Congo (formerly Zaire)	COD	Franc Congolais (formerly New Zaire)	CDF
Denmark	DNK	Danish Krone	DKK
Djibouti	DJI	Djibouti Franc	DJF
Dominica	DMA	E. Caribbean Dollar	XCD
Dominican Rep.	DOM	Dominican Peso	DOP
East Timor	TMP	Timor Escudo	TPE
Ecuador	ECU	Sucre	ECS
Egypt	EGY	Egyptian Pound	EGP
El Salvador	SLV	U.S. Dollar	USD
Equatorial Guinea	GNQ	CFA Franc BEAC	XAF
Eritrea	ERI	Eritrean Nakfa	ERN
Estonia	EST	Kroon	EEK
Ethiopia	ETH	Ethiopian Birr	ETB
European Monetary Cooperation Fund	--	European Currency Unit	XEU
European Union	--	Euro	EUR
Faeroe Is.	FRO	Danish Krone	DKK
Falkland Is. (Malvinas)	FLK	Falkland Is. Pound	FKP
Fiji	FJI	Fiji Dollar	FJD
Finland	FIN	Euro	EUR
France	FRA	Euro	EUR
France Metropolitan	FXX	Euro	EUR
French Guiana	GUF	Euro	EUR
French Polynesia	PYF	CFP Franc	XPF
French Southern Territory	ATF	Euro	EUR
Gabon	GAB	CFA Franc BEAC	XAF

Gambia	GMB	Dalasi	GMD
Georgia	GEO	Georgian Lari	GEL
Germany	DEU	Deutsche Mark	DEM
Ghana	GHA	Cedi	GHC
Gibraltar	GIB	Gibraltar Pound	GIP
Greece	GRC	Euro	EUR
Greenland	GRL	Danish Krone	DKK
Grenada	GRD	E. Caribbean Dollar	XCD
Guadeloupe	GLP	Euro	EUR
Guam	GUM	U.S. Dollar	USD
Guatemala	GTM	Quetzal	GTQ
Guinea	GIN	Guinea Franc	GNF
Guinea—Bissau	GNB	Guinea-Bissau Peso	GWP
Guyana	GUY	Guyana Dollar	GYD
Haiti	HTI	Gourde	HTG
Heard and McDonald Is.	HMD	Australian Dollar	AUD
Holy See (Vatican City State)	VAT	Euro	EUR
Honduras	HND	Lempira	HNL
Hong Kong China	HKG	Hong Kong Dollar	HKD
Hungary	HUN	Forint	HUF
Iceland	ISL	Iceland Krona	ISK
India	IND	Indian Rupee	INR
Indonesia	IDN	Rupiah	IDR
Iran Airlines	--	Iranian Airline Rate	IRA
Iran Islamic Republic of	IRN	Iranian Rial	IRR
Iraq	IRQ	Iraqi Dinar	IQD
Ireland Republic of	IRL	Euro	EUR
Israel	ISR	New Israeli Shekel	ILS
Italy	ITA	Euro	EUR
Jamaica	JAM	Jamaican Dollar	JMD
Japan	JPN	Yen	JPY
Jordan	JOR	Jordanian Dinar	JOD
Kazakhstan	KAZ	Tenge	KZT
Kenya	KEN	Kenyan Shilling	KES
Kiribati	KIR	Australian Dollar	AUD
Korea Democratic People's Republic of (North Korea)	PRK	North Korean Won	KPW
Korea Republic of	KOR	Won	KRW
Kuwait	KWT	Kuwaiti Dinar	KWD
Kyrgyzstan	KGZ	Som	KGS
Lao People's Democratic Republic	LAO	Kip	LAK
Latvia	LVA	Latvian Lats	LVL
Lebanon	LBN	Lebanese Pound	LBP
Lesotho	LSO	Rand	ZAR
Liberia	LBR	Liberian Dollar	LRD
Libyan Arab Jamahiriya	LBY	Libyan Dinar	LYD
Liechtenstein	LIE	Swiss Franc	CHF
Lithuania	LTU	Lithuanian Litas	LTL
Luxembourg	LUX	Euro	EUR
Macau China	MAC	Pataca	MOP
Macedonia the Former Yugoslav Republic of	MKD	Denar	MKD
Madagascar	MDG	Malagasy Franc	MGF

Malawi	MWI	Malawi Kwacha	MWK
Malaysia	MYS	Malaysian Ringgit	MYR
Maldives	MDV	Rufiyaa	MVR
Mali	MLI	CFA Franc BCEAO	XOF
Malta	MLT	Maltese Lira	MTL
Marshall Islands	MHL	U.S. Dollar	USD
Martinique	MTQ	Euro	EUR
Mauritania	MRT	Ouguiya	MRO
Mauritius	MUS	Mauritius Rupee	MUR
Mayotte	MYT	Euro	EUR
Mexico	MEX	Mexican Peso	MXN
Micronesia	FSM	U.S. Dollar	USD
Moldova Republic of	MDA	Moldovan Leu	MDL
Monaco	MCO	Euro	EUR
Mongolia	MNG	Tugrik	MNT
Montenegro		Yugoslavian New Dinar	YUM
Montserrat	MSR	E. Caribbean Dollar	XCD
Morocco	MAR	Moroccan Dirham	MAD
Mozambique	MOZ	Metical	MZM
Myanmar	MMR	Kyat	MMK
Namibia	NAM	Namibia Dollar	NAD
Nauru	NRU	Australian Dollar	AUD
Nepal	NPL	Nepalese Rupee	NPR
Netherlands	NLD	Euro	EUR
Netherlands Antilles	ANT	Nether. Antillian Guilder	ANG
New Caledonia	NCL	CFP Franc	XPF
New Zealand	NZL	New Zealand Dollar	NZD
Nicaragua	NIC	Cordoba Oro	NIO
Niger	NER	CFA Franc BCEAO	XOF
Nigeria	NGA	Naira	NGN
Niue	NIU	New Zealand Dollar	NZD
Norfolk Is.	NFK	Australian Dollar	AUD
Northern Mariana Islands	MNP	U.S. Dollar	USD
Norway	NOR	Norwegian Krone	NOK
Oman	OMN	Rial Omani	OMR
Pakistan	PAK	Pakistan Rupee	PKR
Palau	PLW	U.S. Dollar	USD
Panama	PAN	Balboa	PAB
Papua New Guinea	PNG	Kina	PGK
Paraguay	PRY	Guarani	PYG
Peru	PER	Nuevo Sol	PEN
Philippines	PHL	Philippine Peso	PHP
Pitcairn	PCN	New Zealand Dollar	NZD
Poland	POL	Polish New Zloty	PLN
Portugal	PRT	Euro	EUR
Puerto Rico	PRI	U.S. Dollar	USD
Qatar	QAT	Qatari Rial	QAR
Reunion	REU	Euro	EUR
Romania	ROM	Leu	ROL
Russian Federation	RUS	Russian Ruble (International)	RUB
Russian Ruble (Domestic)	RUS	Russian Ruble (Domestic)	RUR

Rwanda	RWA	Rwanda Franc	RWF
Samoa	WSM	Tala	WST
San Marino	SMR	Euro	EUR
Sao Tome and Principe	STP	Dobra	STD
Saudi Arabia	SAU	Saudi Riyal	SAR
Senegal	SEN	CFA Franc BCEAO	XOF
Seychelles	SYC	Seychelles Rupee	SCR
Sierra Leone	SLE	Leone	SLL
Singapore	SGP	Singapore Dollar	SGD
Slovakia	SVK	Slovak Koruna	SKK
Slovenia	SVN	Tolar	SIT
So. Georgia and So. Sandwich Is.	SGS	Pound Sterling	GBP
Solomon Is.	SLB	Solomon Is. Dollar	SBD
Somalia	SOM	Somali Shilling	SOS
South Africa	ZAF	Rand	ZAR
Spain	ESP	Euro	EUR
Sri Lanka	LKA	Sri Lanka Rupee	LKR
St. Helena	SHN	St. Helena Pound	SHP
St. Kitts-Nevis	KNA	E. Caribbean Dollar	XCD
St. Lucia	LCA	E. Caribbean Dollar	XCD
St. Pierre and Miquelon	SPM	Euro	EUR
St. Vincent and The Grenadines	VCT	E. Caribbean Dollar	XCD
Sudan	SDN	Sudanese Pound	SDD
Sudan Airlines	--	Sudan Airline Rate	SDA
Suriname	SUR	Surinam Guilder	SRG
Svalbard and Jan Mayen Is.	SJM	Norwegian Krone	NOK
Swaziland	SWZ	Lilangeni	SZL
Sweden	SWE	Swedish Krona	SEK
Switzerland	CHE	Swiss Franc	CHF
Syrian Arab Rep.	SYR	Syrian Pound	SYR
Taiwan	TWN	New Taiwan Dollar	TWD
Tajikistan	TJK	Somoni	TJS
Tanzania United Republic of	TZA	Tanzanian Shilling	TZS
Thailand	THA	Thailand Baht	THB
Togo	TGO	CFA Franc BCEAO	XOF
Tokelau	TKL	New Zealand Dollar	NZD
Tonga	TON	Pa'anga	TOP
Trinidad and Tobago	TTO	Trinidad and Tobago Dollar	TTD
Tunisia	TUN	Tunisian Dinar	TND
Turkey	TUR	Turkish Lira	TRL
Turkmenistan	TKM	Manat	TMM
Turks and Caicos Is.	TCA	U.S. Dollar	USD
Tuvalu	TUV	Australian Dollar	AUD
U.S. Minor Outlying Islands	UMI	U.S. Dollar	USD
U.S. Virgin Is.	VIR	U.S. Dollar	USD
Uganda	UGA	Uganda Shilling	UGX
Ukraine	UKR	Ukrainian Hryvnia	UAH
United Arab Emirates	ARE	U.A.E. Dirham	AED
United Kingdom	GBR	Pound Sterling	GBP
United States	USA	U.S. Dollar	USD
Uruguay	URY	Peso Uruguayo	UYU

Uzbekistan	UZB	Uzbekistan Sum	UZS
Vanuatu	VUT	Vatu	VUV
Venezuela	VEN	Bolivar	VEB
Vietnam	VNM	Dong	VND
Wallis and Futuna Is.	WLF	CFP Franc	XPF
Western Sahara	ESH	Moroccan Dirham	MAD
Yemen	YEM	Yemeni Rial	YER
Yugoslavia	YUG	Yugoslavian New Dinar	YUM
Zambia	ZMB	Zambian Kwacha	ZMK
Zimbabwe	ZWE	Zimbabwe Dollar	ZWD