CyberSource International

Secure Acceptance Web/Mobile Implementation

Bank Muscat

i. Documentation Versions

This table lists the versioning of this document to date:

Date	Version	Author
6 January 2013	1.0	Karun Malhotra
7 April 2013	2.1	Karun Malhotra
24 April 2013	2.2	Karun Malhotra

ii. Confidential Information

All material contained in this document is confidential information. The confidential information may not be disclosed to third parties other than employees and authorized contractors on behalf of Bank Muscat and/or CyberSource.

iii. CyberSource Contact Information

For general information about our company, products and services, go to http://www.cybersource.com

Contents

1. Introduction to Secure Acceptance

1.1. What Is It?

The Secure Acceptance is the easiest and fastest way to accept credit cards and verify payments on a web store by adding a few lines of text to a website. After the customer places an order through Secure Acceptance, it can be viewed in the CyberSource Enterprise Business Centre, a central online management portal for supervising all the online payment transactions.

CyberSource Secure Acceptance solution also supports many types of mobile devices, such as Apple iPhone/iPad, BlackBerry, Nokia, Google Android etc; and has the ability to adjust the payment pages according to the screen size of the device automatically with no additional coding effort.

Secure Acceptance is fully hosted by CyberSource therefore the payment data needs of the customer are not handled directly by the merchant. This significantly helps in decreasing the Payment Card Industry Data Security Standard (PCI-DSS) obligations that merchants face when processing Card-Not-Present type transactions.

Please visit https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml for more information regarding PCI-DSS regulations.

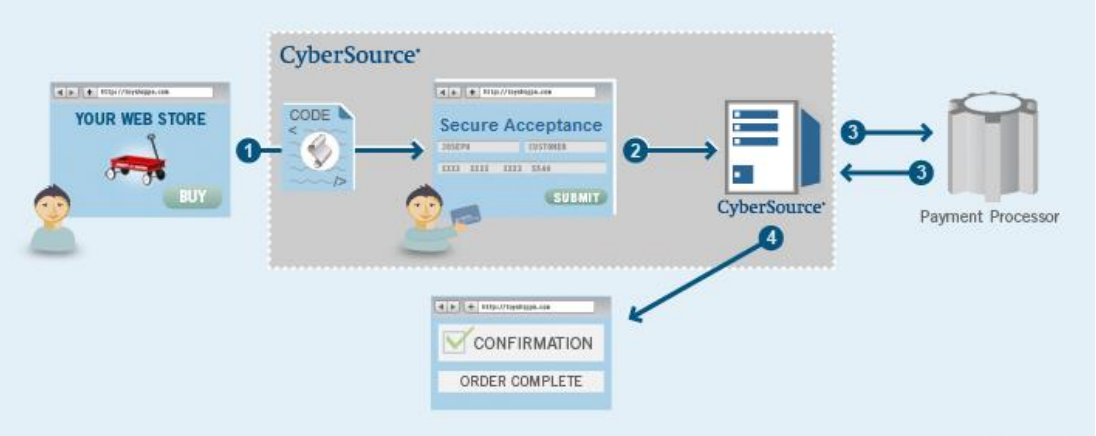
Should you have any further enquiries or have specific questions around PCI-DSS compliancy, then please email vpssais@visa.com who will be able to advise.

1.2. Benefits & Advantages

The main advantages of using Secure Acceptance Web/Mobile are:

- **Security Compliance** – hosted services mean faster and easier to achieve PCI-DSS certification
- **Reduced Risk** – no handling or storage of sensitive customer account data
- **Low Maintenance** – leave compliance and order page maintenance to CyberSource
- **Speed** – faster and easier than implementing in-house order pages, especially if accepting online orders quickly is required
- **Customisation** – customise basic visual elements and messaging for customers
- **Virtually Transparent** – customers move seamlessly from web store to CyberSource's Secure Acceptance pages & back to webstore/confirmation page
- **Language Support** – provide customers with checkout pages translated into their native language (Over 25 languages included including Arabic)
- **Mobile Acceptance** – single integration, many channels of payment acceptance handled
- **Automatic** – customers input their own order information
- **Easy Order Management** – online Business Centre (portal) to review and manage all orders from any computer with Internet access

1.3. How It Works



Step 1

With minor modifications pasted into the website, the web store will forward customers who are ready to check out to a hosted, PCI-compliant order form. (There are options to customise the basic content and look of Secure Acceptance, but CyberSource provide a default setup to get started. The setup includes the information required for customers to provide when they place an order.) When the customer clicks 'Buy' on the website, they are forwarded to the Secure Acceptance payment pages where they enter their own payment details. Transition to this Secure Acceptance solution is virtually transparent to the customer.

Step 2
From the Secure Acceptance, the customer clicks 'Submit' to confirm their purchase, and the order information enters CyberSource's system.

Step 3
CyberSource sends a request for approval to VisaNet in real-time. VisaNet then sends a reply via CyberSource containing order & payment information.

Step 4
The reply information is used to display a message to the customer about whether the order was approved. The reply can also include other information, such as payment information and billing & shipping address details, including 3DSecure and fraud screening information in some circumstances.

Conclusion
The order can be viewed in the Business Centre, a central location for managing online payment transactions. Approved transactions can be automatically submitted for settlement or an order may be designated to be submitted for funding as the goods are shipped.

2. Prerequisite Implementation Requirements

2.1. Technical Requirements

To use Secure Acceptance, merchants **must** be able to create web pages that will gather customer and order information (excluding card data) for payment and fraud screening services into requests and merchants must be able to process the reply information to fulfil the customer's order.

Merchants must meet the following requirements:

- basic shopping-cart software or bespoke shopping website
- an ISP hosts merchants product pages in one of the supported scripting languages
- web store may have a secure (SSL) order form

2.2. Web Developers

The merchants must exhibit basic programming skills in one of the following supported programming languages in order to implement the CyberSource Secure Acceptance:

- Ruby
- PHP
- Perl
- JSP
- VB
- .NET (C#)

Please note, no other programming languages other than those mentioned above in Section 2.2 may be used. The above languages are fully supported by CyberSource. Should a merchant use another programming language outside of this list, this will not be supported.

2.3. Support JavaScript

The CyberSource Secure Acceptance requires the customer's browser to support and have **enabled JavaScript** in order to operate correctly.

3. Registering Test Accounts

For more information or advice in creating CyberSource Merchant ID (MID) and the naming convention, please contact your Bank Muscat Account Manager.

3.1. Registering Test Accounts

In order to utilise the CyberSource payment gateway services, all merchants are required to obtain a CyberSource test Merchant ID for integration and testing.

Please contact your Bank Muscat Account Manager who will be able to provide further guidance on how to obtain a test account.

3.2. Activating Services

Once registration of the Merchant's CyberSource Merchant ID has been successful, Bank Muscat will raise an "**Enabling Services**" request. The request will include the Merchant ID and the services required which will be payments processing, the currencies and/or Decision Manager. Please speak with your Bank Muscat Account representative to enable the required services.

4. Implementation of Secure Acceptance

Payment transactions have two predetermined process flows through CyberSource, either with or without the Decision Manager fraud monitoring solution. It is strongly advised that these flows are understood before proceeding with the implementation. These flow diagrams can be found in Appendix A – Process Flows.

Please contact your Bank Muscat Account Manager with any further clarifications.

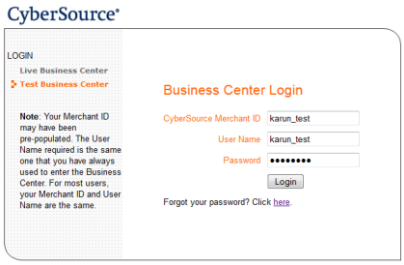
4.1. Step-by-Step Configuration

Before being able to deploy and send transactions via Secure Acceptance, the solution needs to be tailored and configured to the merchant's requirements using the below Step-By-Step Configuration Guide:

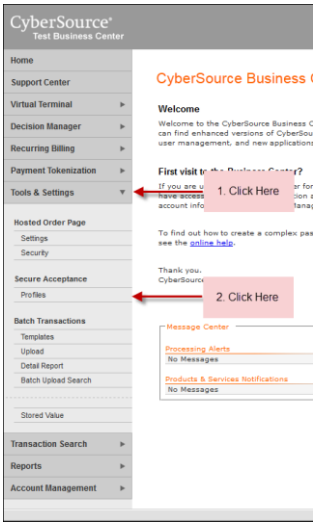
1. Login to the Enterprise Business Centre (EBC)
    a. Open a web browser** and navigate to https://ebctest.cybersource.com
    b. Enter your CyberSource Merchant ID *
    c. Enter your Username *
    d. Enter your Password *
    e. Click Login button and accept the notification of being in the TEST environment

    *** Provided by your Bank Muscat Account Manager**

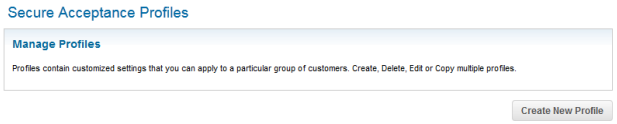
    ****supported browsers are Internet Explorer and FireFox**



2. Once logged in, Click "Tools & Settings" on the left-hand menu followed by "Profiles" under the "Secure Acceptance" heading



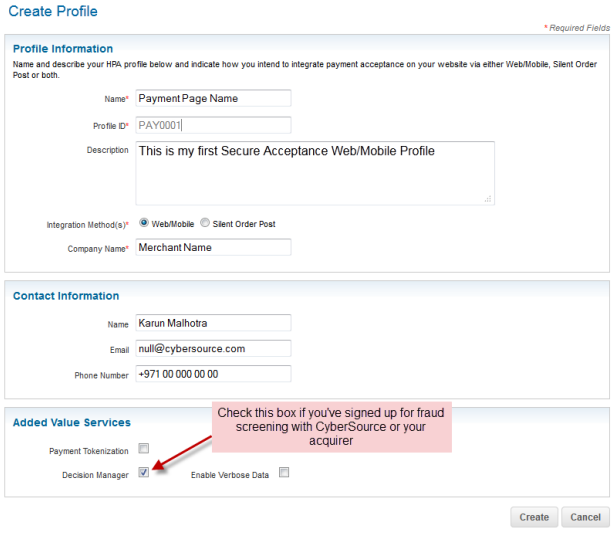
3. Click “Create New Profile” Button



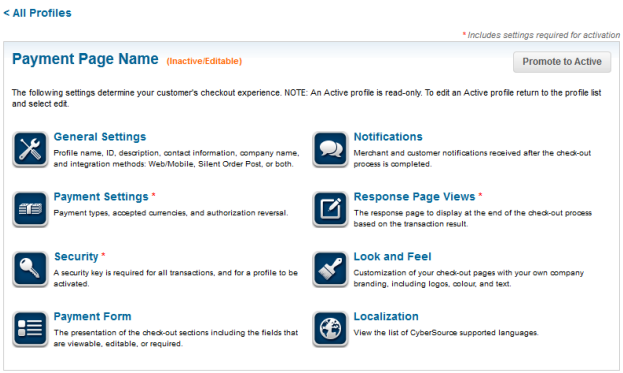
4. Populate the form as per the screenshot. Mandatory fields are denoted by a red asterisks. Click the “Create” button once completed.

Please note the following:
Name – max 20 alphanumeric characters
Profile ID – 7 alphanumeric characters exactly. It is used in every transaction.
Description – max 255 characters
Company Name – max 40 characters

Note: please ensure valid contact information is entered.



5. If successfully created, the settings menu will be displayed. Click the “Payment Settings”.

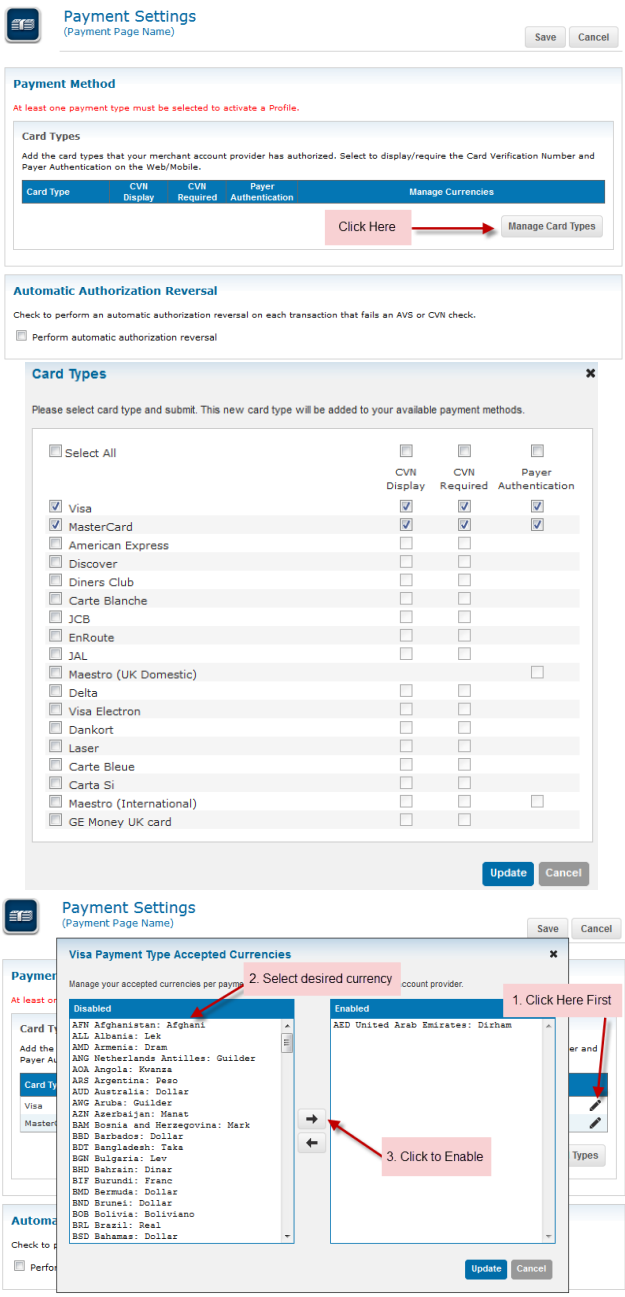


6. As default, no payment types are selected. In order to accept a card type, click the “Manage Card Types” button.
   Select the card types you wish to accept and supported by your acquirer. It is advised you display and require Card Verification Number (CVN); as well as Payer Authentication (3DSecure). Click the “Update” button once complete.

   Check the “Perform automatic authorisation reversal” box should you wish to unreserved a customer’s funds from their bank account in the even AVS or CVN fail.

7. Following selection of payment types, currencies per payment type need to be configured. Click the Pencil icon for each and select desired currency across to “Enabled”. Click the “Update” button once complete.

8. Once all desired payment types and currencies are configured click the “Save” button.



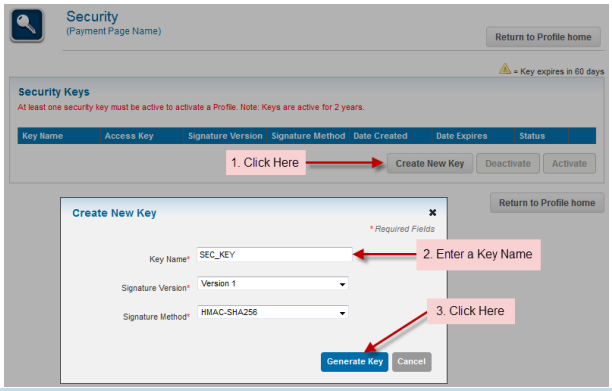
9. At the Profile Settings Menu, click the “Security” button.

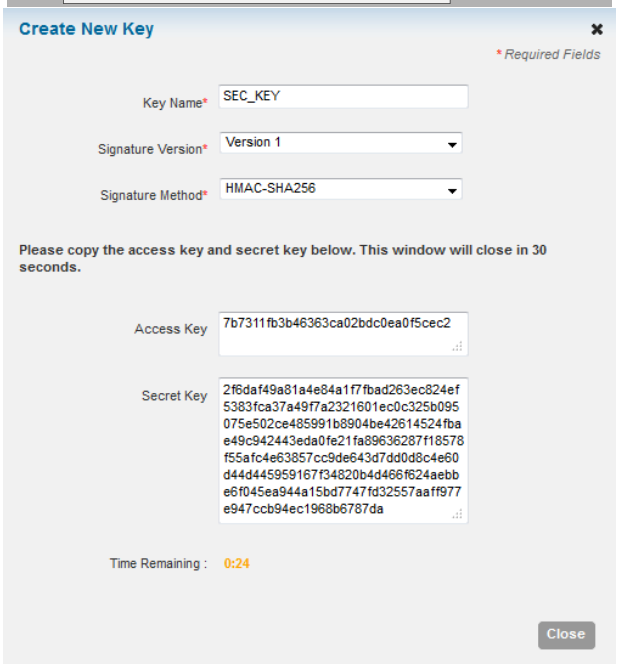
   Click the “Create New Key” button to generate a Security Key for your Secure Acceptance profile.

   Give the New Key a name and click the “Generate Key” button.

10. The lightbox will expand to show your Secure Acceptance “Access Key” and “Secret Key”. **These will be displayed for 30 seconds before disappearing,** copy both into a safe location or Notepad for the time being, both keys will be required during implementation of the code (See Section 4.2 of this document).

    It is possible to view these keys again by clicking the key in the Security Key table.



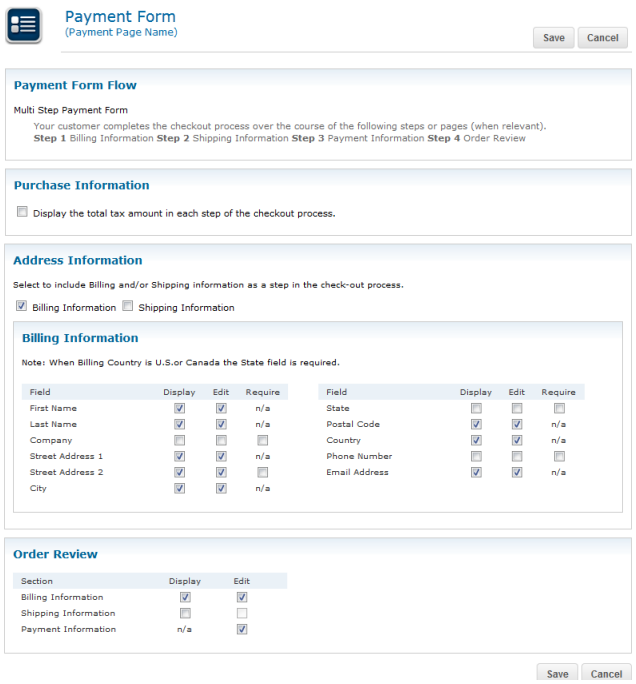


11. At the Profile Settings Menu, click the “Payment Form” button.

    The screenshot showcases the default fields to be displayed in the Secure Acceptance payment pages and can be customised to suit the checkout flow.

    Should the billing and/or shipping address be captured at an earlier stage of the order process (e.g. on the merchant’s website), these fields can be passed in hidden form fields (See Section 4.5 of this document).

    Click the “Save” button when complete.

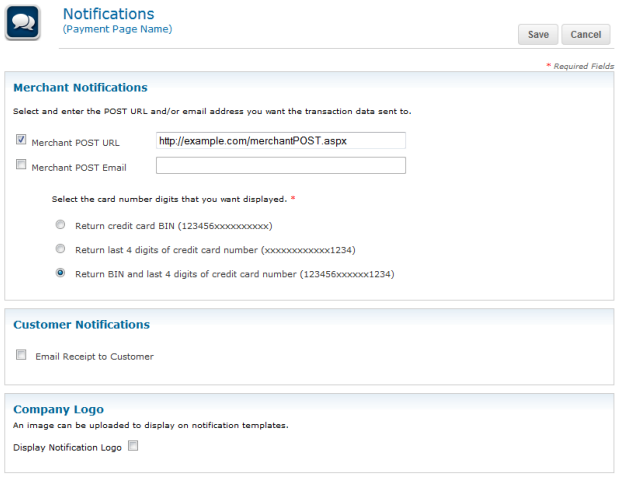


12. At the Profile Settings Menu, click the “Notifications” button.

    It is strongly advised to implement the Merchant POST URL to receive notification of each transaction from CyberSource into the merchant systems (e.g. order management system). The merchant would need to programmatically capture the response sent to this URL and store them within their systems. This will ensure accuracy of transactions and give the merchant visibility.

    Please note – use port 80, 443 or 8080.

    Click the “Save” button when complete.

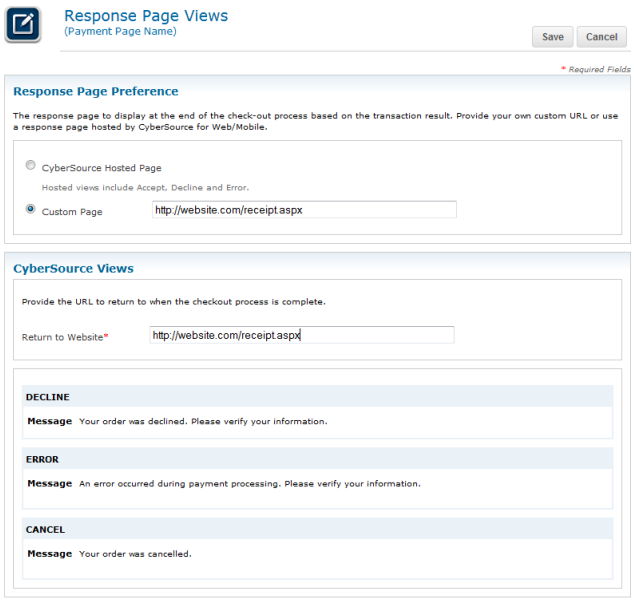


13. At the Profile Settings Menu, click the “Response Page Views” button.

    By default, the use of CyberSource’s own response pages is selected “CyberSource Hosted Page”; however CyberSource recommends implementing a custom page where the responses is interpreted and displayed to the customer for the following Transaction Decisions:

    - Accept
    - Decline
    - Error
    - Cancel

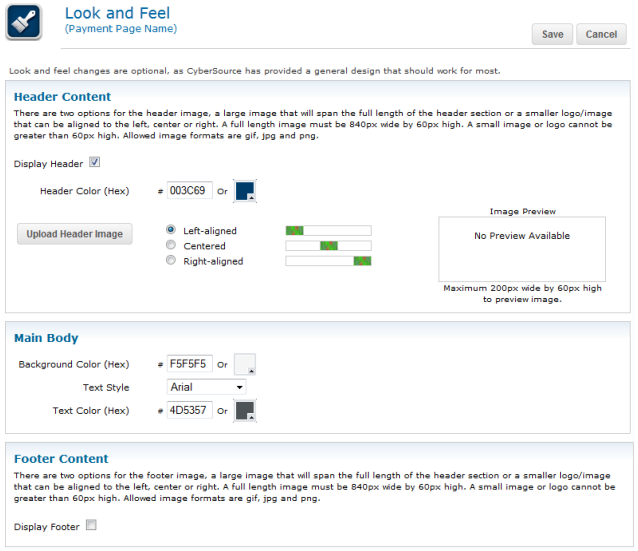
    Click the “Save” button when complete.



14. At the Profile Settings Menu, click the “Look and Feel” button.

    By default, CyberSource has pre-configured the “Header” and “Body” of the Secure Acceptance payment pages. It is possible to change the colours, aligned or upload an image of the Header, Body and Footer.

    Click the “Save” button when complete.



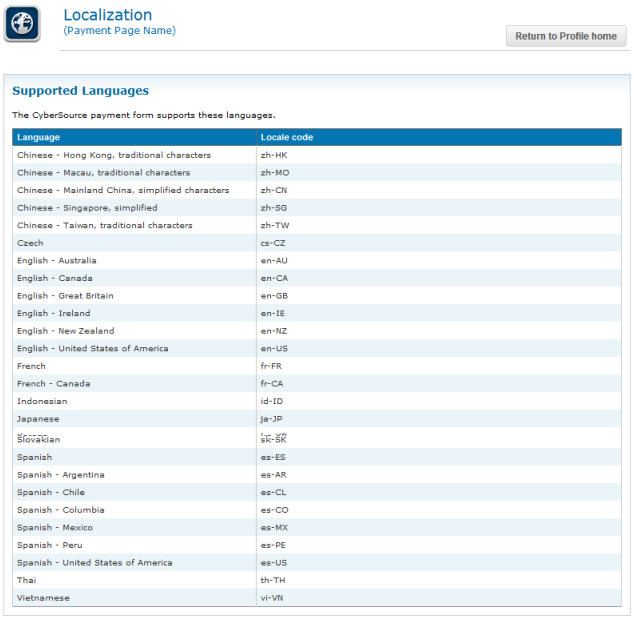
15. At the Profile Settings Menu, click the “Localization” button.

    Showcases the possible languages supported through Secure Acceptance Web/Mobile; the Locale Code can be utilised within the website code to initiate Secure Acceptance.

    e.g.

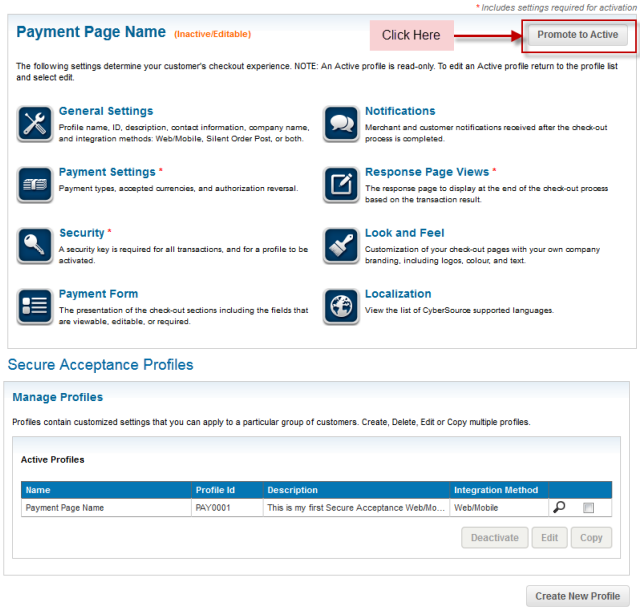
    ```
    <input type="hidden"
    name="locale"
    value="en-us">
    ```

    Click the “Return to Profile home” button.



16. At the Profile Settings Menu, once all settings have been configured satisfactorily; click the “Promote to Active” button.

    This locks the Profile so that cannot be edited while it is in use on a website; unless it is explicitly deactivated or copied.



4.2. Development of Secure Acceptance

By utilising one of the supported languages, Secure Acceptance Web/Mobile can be implemented very quickly by using and modifying the sample scripts provided by CyberSource (See Section 4.3 of this document for links to those examples).

Each example is provided with the following files:

- Security script
- Payment form
- Payment confirmation page
- Receipt page

4.2.1. Modifying the Security Script

The security script only needs to be modified by including the Secret Key generated at point 10 of Section 4.1 of this document. In the PHP example, this change will look like:

```
define ('SECRET_KEY', '
2f6daf49a81a4e84a1f7fbad263ec824ef5383fca37a49f7a2321601ec0c32
5b095075e502ce485991b8904be42614524fbae49c942443eda0fe21fa8963
6287f18578f55afc4e63857cc9de643d7dd0d8c4e60d44d445959167f34820
b4d466f624aebbe6f045ea944a15bd7747fd32557aaff977e947ccb94ec196
8b6787da');
```

4.2.2. Modifying the Payment Form

The payment form represents the checkout basket of an e-Commerce site. For the purpose of the example of Secure Acceptance, some fields are shown that would very well be hidden from view of a customer and passed through in the POST message.

In the PHP example, the minimum that needs to be changed are the Access Key and Profile ID (as generated/created in Section 4.1 of this document):

```
<input type="hidden" name="access_key" value="
7b7311fb3b46363ca02bdc0ea0f5cec2">

<input type="hidden" name="profile_id" value="PAY0001">
```

4.2.3. Modifying the Payment Confirmation Page

The payment confirmation page represents the review of the basket prior to proceeding with making a payment. For the purpose of the example of Secure Acceptance, all fields and data is shown prior to the POST message being made to CyberSource.

In the PHP example, the minimum that needs to be changed is the POST form URL for either TEST or PRODUCTION:

Environment	URL
TEST	`<form action="https://testsecureacceptance.cybersource.com/pay" method="post" />`
PRODUCTION	`<form action="https://secureacceptance.cybersource.com/pay" method="post" />`

4.3. Example Secure Acceptance/Implementations

CyberSource provides a number of examples in a variety of languages for the merchant to get started with their implementation of the Secure Acceptance.

The supported development languages are:

- Perl
- PHP
- VB
- .NET (C#)
- JSP
- Ruby

Please see Appendix B – Example Code for examples of the Secure Acceptance Web/Mobile.

4.4. UTF-8

For merchants wishing to capture the Billing Information prior to initiating Secure Acceptance Web/Mobile, CyberSource recommends merchants ensure all encoding is UTF-8 compliant.

This will ensure successful authentication of transactions containing non-ANSII character sets, for example Arabic or Cyrillic; providing customers the flexibility to enter their information in familiar format.

4.5. Device Fingerprinting

In order to successfully implement Device Fingerprinting, a 1-pixel image file (which cannot be seen) and two scripts need to be placed in the <body> tag of Merchants checkout page at the top of the main body. This will ensure a 3-5 second window in which the code segments can complete the data collection necessary to create a fingerprint for the device making the order.

Below are the code segments for implementing Device Fingerprinting:

PNG Image

<p style="background:url(https://h.online-metrix.net/fp/clear.png?org_id=***<org ID>***&session_id=***<merchant id><session ID>***&m=1)"></p> <img src="https://h.online-metrix.net/fp/clear.png?org_id=***<org ID>***&session_ id=***<merchant id><session ID>***&m=2" alt="">

Flash Code

<object type="application/x-shockwave-flash" data="https://h.online-metrix.net/fp/ fp.swf?org_id=***<org ID>***&session_id=***<merchant id><session ID>***" width="1" height="1" id="thm_fp"> <param name="movie" value="https://h.online-metrix.net/fp/fp.swf?org_id=***<org ID>***&session_id=***<merchant id><session ID>***" /> </object>

JavaScript Code

<script src="https://h.online-metrix.net/fp/check.js?org_id=***<org ID>***&session_ id=***<merchant id><session ID>***" type="text/javascript"> </script>

The following attributes need to be placed within the italic bold sections of the above code segments:

- Domain:
  - Testing – Use *h.online-metrix.net*, which is the DNS name of the fingerprint server as shown in the sample HTML tags above.
  - Production – Change the domain name to a local URL, and configure Merchants Web server to redirect the URL to *h.online-metrix.net*
- <org ID>:

Test Org ID:	1snn5n9w
Live Org ID:	k8vif92e

- <merchant ID>: Merchants unique CyberSource merchant ID
- <session ID>: The session ID is a string variable (letters and numbers only) that must be unique for each merchant ID. Merchants can use any string that they are already generating, such as an order number or Web session ID. However, **do not use** the same uppercase and lowercase letters to indicate different session IDs.

4.6. Required & Optional Fields

Below is a list of required and Optional fields required for payments processing and fraud screening with CyberSource/Bank Muscat. A full and extensive list of fields can be found in the Secure Acceptance Web/Mobile User's Guide (Page 39).

Field Name	Description	Required or Optional	Data Type (Length)
access_key	Authentication with Secure Acceptance	R	String (32)
amount	Total amount for the order. Must be greater than or equal to zero and must equal the total amount of each line item	R	String (15)
currency	Currency used for the order (ISO Currency Codes)	R	String (5)
locale	Indicates the language to use for customer-facing content	R	String (5)
profile_id	Identifies the profile to use with each transaction	R	String (7)
reference_number	Unique merchant-generated order reference or tracking number for each transaction	R	String (60)
signature	Merchant-generated Base64 signature. This is generated using the signing method for the access_key field supplied.		
signed_date_time	The date and time that the signature was generated. Must be in UTC Date & Time format. This field is used to check for duplicate transaction attempts.	R	String (20)
signed_field_names	A comma-separated list of request fields that are signed. This field is used to generate a signature that is used to verify the content of the transaction to protect it from tampering. **Important** CyberSource recommends signing **all** request fields except the signature field.	R	Variable
transacation_type	The type of transaction: - authorization - **sale** (combined auth & settle)	R	String (60)
transaction_uid	Unique merchant-generated identifier. Include with the access_key field for each transaction. This identifier must be unique for each transaction. This field is used to check for duplicate transaction attempts.	R	String (50)
unsigned_field_names	A comma-separated list of request fields that are not signed.	R	Variable
bill_to_address_city	City in the billing address	O/R *	String (50)

bill_to_address_country	Country code for the billing address (ISO Country Codes)	O/R *	String (2)
bill_to_address_line1	First line of the billing address	O/R *	String (60)
bill_to_address_postal_code	Postal code for the billing address	O/R *	String (10)
bill_to_address_state	State or province in the billing address (ISO State & Province Code)	O/R *	String (2)
bill_to_email	Customer's email address, including the full domain name	O/R *	String (255)
bill_to_forename	Customer's first name. This name must be the same as the name on the card	O/R *	String (60)
bill_to_phone	Customer's phone number	O/R *	String (15)
bill_to_surname	Customer's last name. This name must be the same as the name on the card	O/R *	String (60)
device_fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_). However, do not use the same uppercase and lowercase letters to indicate different session IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID.	O	String (88)
ignore_avs	Ignore the results of AVS verification. Possible values: - true - false **Important** To prevent data tampering, CyberSource recommends signing this field. Only applicable for order from UK, USA or Canada; otherwise can be ignored.	O	String (5)
ignore_cvn	Ignore the results of CVN verification. Possible values: - true - false **Important** To prevent data tampering, CyberSource recommends signing this field.	O	String (5)
item_#_name	Name of the item. # can range from 0-49	O	String (255)
item_#_quantity	Quantity of line items. # can range from 0-49	O	String (10)
item_#_sku	Identification code for the product. # can range from 0-49	O	String (255)
item_#_unit_price	Price of the line item. # can range from 0-49	O	String (15)
line_item_count	Total number of line items. Maximum number is 50	O	String (2)

payment_method	Method of payment: card	R	String (30)
ship_to_address_city	City of shipping address	O	String (50)
ship_to_address_country	Country code for the shipping address (ISO Country Codes)	O	String (2)
ship_to_address_line1	First line of shipping address	O	String (60)
ship_to_address_postal_code	Postal code for the shipping address	O	String (10)
ship_to_address_state	State or province of shipping address (ISO State & Province Code)	O	String (2)
ship_to_forename	First name of the person receiving shipment	O	String (60)
ship_to_phone	Phone number of the shipping address	O	String (15)
ship_to_surname	Last name of the person receiving the shipment	O	String (60)

* These fields are mandatory with every transaction request; however a merchant has the ability to optionally POST these to Secure Acceptance, through hidden fields or otherwise. For example, a merchant does not wish to utilize the Secure Acceptance Billing Information page to collect this information, therefore utilized the fields mentioned above in the POST request.

4.7. Merchant Defined Data (MDD) Fields

Transaction requests have the ability to be sent with additional data, also known Custom Fields, to aid in fraud prevention employed at Bank Muscat. The field name is “merchant_defined_data#” where the # is replaced with a value between 1-100.

Required fields should be sent in hidden fields via the request POST message: <input type=”hidden” name=”merchant_defined_data1” value=”TEST”>

For a complete list of fields required per transaction based upon the merchant type, please contact Bank Muscat.

4.8. Reason Code & Decision

CyberSource provide a number of response fields related to each request submitted, the most important of them are “reason_code” and “decision”. The decision field will give notification of the overall status of the transaction process, encompassing all services (Payment, Payer Authentication and Decision Manager). This field should be used and interpreted into a customer friendly message, either declining or accepting their transaction.

There are four possible outcomes for this field:

- ACCEPT
- REJECT
- REVIEW *
- ERROR

* Review decision will only be seen if Decision Manager is being used and a review process is in place to handle these transaction cases.

The reason code field can be used to provide a merchant more background of a transaction status and are directly mapped to the appropriate decision.

Decision	Reason Code
ACCEPT	100, 110
REVIEW	200, 201, 230, 480, 520
REJECT	102, 200, 202, 203, 204, 205, 207, 208, 210, 211, 221, 222, 230, 231, 232, 233, 234, 236, 240, 475, 476, 481
ERROR	104, 150, 151, 152, 250

These reason codes are fully described in Appendix C – Reason Codes of this document.

5. Testing

5.1. How to Test Secure Acceptance

It is recommended to test the implementation of the Secure Acceptance extensively; CyberSource provides the below mandatory details that can be used for testing:

- First Name – noreal
- Last Name – name
- Street 1 – 1295 Charleston Road
- City – Mountain View
- State - CA
- Postal Code – 94043
- Country – US
- Email – null@cybersource.com

Please use the following test card numbers:

Visa – 4111 1111 1111 1111
MasterCard – 5555 5555 5555 4444
JCB – 3566 1111 1111 1113
American Express – 3782 8224 6310 005

In addition, CyberSource provides a number of test cases which can be used to verify the handling of response data for all eventualities/scenarios that may arise during production e-commerce processing. Please use the following links:

Authorisation Testing
AVS Testing
CAVV Testing
CVV Testing
Error Testing
Reject Codes Testing

6. Go-Live Procedure

6.1. How to Request a Go-Live

When the merchant is ready to implement Secure Acceptance in their live environment, Bank Muscat will need to request Go-Live with CyberSource on behalf of the merchant.

Please note that Go-Live requests can take upto **Seven UK Working Days** to action and no Go-Live will take place on Fridays.

6.2. Testing in Production

CyberSource recommends testing the implementation of Secure Acceptance in the production environment prior to fully releasing it to the general public.

In order to do this, the merchant will be required to use a **real valid credit** card with the associated billing details to the card. The merchant will then be able to verify the implementation and reverse the charge or refund through the CyberSource Enterprise Business Centre.

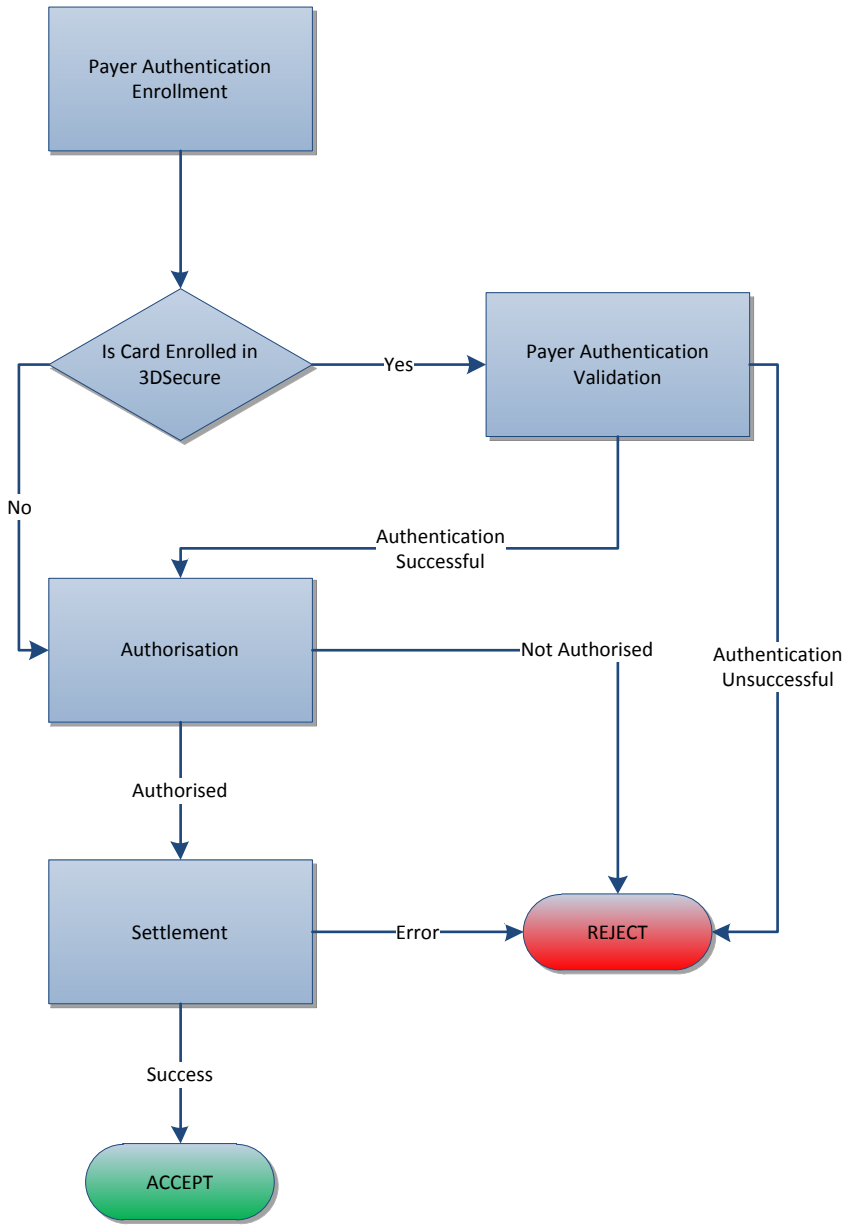
NO DUMMY OR TEST DATA MAY BE USED TO PERFORM TESTS IN PRODUCTION

7. Additional Information

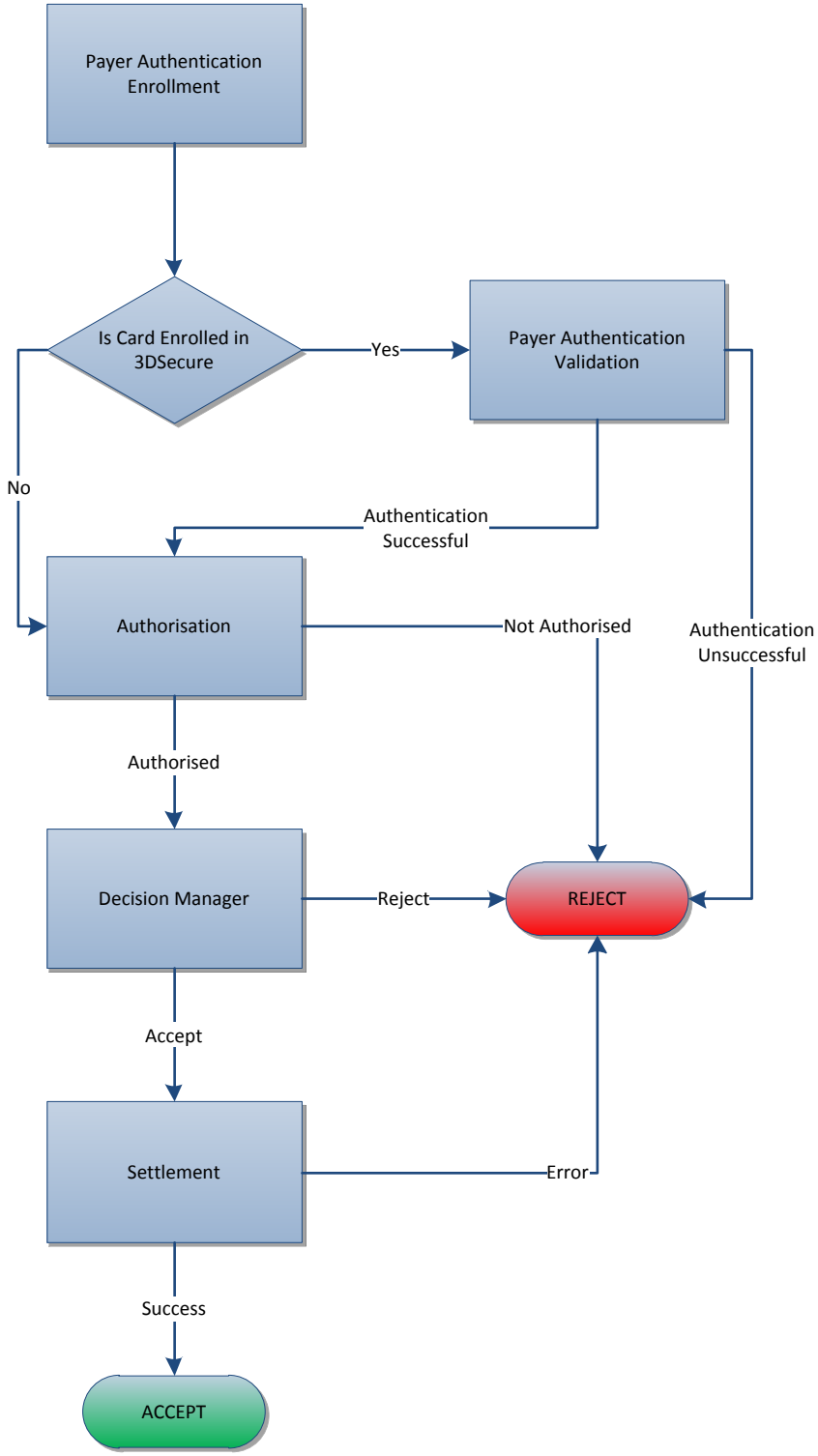
CyberSource Business Center	Test - https://ebctest.cybersource.com Live – https://ebc.cybersource.com
CyberSource Account Registration	http://www.cybersource.com/register
CyberSource Support Center/Knowledgebase	https://support.cybersource.com
Secure Acceptance Web/Mobile User's Guide	Secure_Acceptance_WM.pdf
Enterprise Business Centre Overview	EBC_Overview.pdf
Business Centre Tutorial	Business Centre Tutorial.html

Appendix A – Process Flows

Payments Only



Payments & Decision Manager



Appendix B – Example Code

PHP	http://apps.cybersource.com/library/documentation/dev_guides/samples/sa_sc/php.zip
VB	http://apps.cybersource.com/library/documentation/dev_guides/samples/sa_sc/vb.zip
Perl	http://apps.cybersource.com/library/documentation/dev_guides/samples/sa_sc/perl.zip
JSP	http://apps.cybersource.com/library/documentation/dev_guides/samples/sa_sc/jsp.zip
Ruby	http://apps.cybersource.com/library/documentation/dev_guides/samples/sa_sc/ruby.zip
.NET	http://apps.cybersource.com/library/documentation/dev_guides/samples/sa_sc/csharp.zip

Appendix C – Reason Codes

Reason Code	Description
100	Successful transaction
101	The request is missing one or more required fields
102	One or more fields in the request contains invalid data
110	Only a partial amount was approved
150	General system failure
151	The request was received but there was a server timeout. This error does not include timeouts between the client and the server. Possible Action – to avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Enterprise Business Centre
152	The request was received, but a service did not finish running in time Possible Action – to avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Enterprise Business Centre
200	The authorisation request was approved by the issuing bank but declined by CyberSource because it did not pass the Address Verification System (AVS) check Possible Action – you can capture the authorisation, but consider reviewing the order for the possibility of fraud
201	The issuing bank has questions about the request. You do not receive an authorisation code programmatically, but you might receive one verbally by calling the processor. Possible Action – call your processor to possibly receive a verbal authorisation. For contact phone numbers, refer to Bank Muscat
202	Expired card. You might also receive this if the expiration date you provided does not match the date the issuing bank has on file. Possible Action – request a different card or other form of payment
203	General decline of the card. No other information was provided by the issuing bank. Possible Action – request a different card or other form of payment
204	Insufficient funds in the account. Possible Action – request a different card or other form of payment
205	Stolen or lost card. Possible Action – review this transaction manually to ensure that you submitted the correct information
207	Issuing bank unavailable. Possible Action – wait a few minutes and resend the request
208	Inactive card or card not authorised for card-not-present transactions. Possible Action – request a different card or other form of payment
209	American Express Card Identification Digits (CID) did not match Possible Action – request a different card or other form of payment
210	The card has reached the credit limit. Possible Action – request a different card or other form of payment

211	Invalid CVN. Possible Action – request a different card or other form of payment
221	The customer matched an entry on the processor's negative file. Possible Action – review the order and contact Bank Muscat
230	The authorisation request was approved by the issuing bank but declined by CyberSource because it did not pass the CVN check. Possible Action – you can capture the authorisation, but consider reviewing the order for the possibility of fraud
231	Invalid account number. Possible Action – request a different card or other form of payment
232	The card type is not accepted by the payment processor. Possible Action – contact Bank Muscat to confirm that merchant account is setup to receive the card in question
233	General decline by the processor. Possible Action – request a different card or other form of payment
234	There is a problem with the information in your CyberSource account. Possible Action – do not resend the request. Contact Bank Muscat to correct the information in your account
235	The requested capture amount exceeds the originally authorised amount. Possible Action – issue a new authorisation and capture request for the new amount
236	Processor failure. Possible Action – wait a few minutes and resend the request
237	The authorisation has already been reversed. Possible Action – no action required
238	The authorisation has already been captured. Possible Action – no action required
239	The requested transaction amount must match the previous transaction amount. Possible Action – correct the amount and resend the request
240	The card type send is invalid or does not correlate with the credit card number. Possible Action – confirm that the card type correlates with the credit card number specified in the request, then resend the request
241	The request ID is invalid. Possible Action – request a new authorisation, and if successful, proceed with the capture

242	You requested a capture, but there is no corresponding, unused authorisation record. Occurs if there was not a previously successful authorisation request or if the previously successfully authorisation has already been used by another capture request. Possible Action – request a new authorisation, and if successful, proceed with the capture
243	The transaction has already been settled or reversed. Possible Action – no action required
246	One of the following: ▪ The capture or credit is not voidable because the capture or credit information has already been submitted to your processor Or ▪ You requested a void for a type of transaction that cannot be voided Possible Action – no action required
250	The request was received, but there was a timeout at the payment processor. Possible Action – to avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Enterprise Business Centre
254	Stand-alone credits are not allowed. Possible Action – submit a follow-on credit by including a request ID in the credit request. A follow-on credit must be requested within 60 days of the authorisation. To process stand-alone credits, contact Bank Muscat account manager to find out if this is supported for your account
400	The fraud score exceeds Bank Muscat threshold Possible Action – review the customer's order
476	The customer cannot be authenticated Possible Action – review the customer's order
480	The order is marked for review by Decision Manager Possible Action – Hold the customer's order and contact Bank Muscat for further guidance
481	The order is rejected by Decision Manager Possible Action – do not proceed with customer's order

This page is intentionally left blank