Payment Gateway Specification

Developer Guide

Document No: 0002

Version 1.2

Qualpay Inc | San Mateo, CA 94402 | 1 844 282 0888

Qualpay contact information

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

For sales questions about any Qualpay, email sales@qualpay.com
or call 1 844 282 0888.

For Customer Service or integrations questions about any Qualpay, email
support@qualpay.com or call 1 844 282 0888.

Copyright

Notice of non-liability

Revision History

Revision	Date	Reference Id	Summary of Change
1.0	08/01/14		Initial Revision
1.1	10/23/14		Added sections for Retry and CORS Support
1.2	01/14/15		Simulator changes

Table of Contents

1. ABOUT THIS MANUAL

1.1 Overview

The purpose of this document is to describe the Qualpay Payment Gateway RESTful API. It details the commands available to developers and includes examples to assist during the integration and certification process.

1.2 Conventions

Valid field names will appear *italicized* in this manual. Field names framed by <> characters indicate that the merchant should provide the appropriate field data. For example, a value of *<pg_id>* indicates that the merchant should provide the *pg_id* that the message is referencing.

2. MESSAGE TYPES

2.1 Overview

This chapter provides a description of the available message types.

2.2 Authorization

An authorization message is used to send cardholder data to the issuing bank for approval. An approved transaction will continue to be open until it expires or a capture message is received. Authorizations are automatically voided if they are not captured within 28 days, although most issuing banks will release the hold after 24 hours in retail environments or 7 days in card not present environments.

URL: https://api.qualpay.com/pg/auth

2.3 Verify

A verify message is used to send cardholder data to the issuing bank for validation. A verify message will return success if the cardholder information was verified by the issuer. If the AVS or CVV2 field is included in the message, then the AVS or CVV2 result code will be returned in the response message.

URL: https://api.qualpay.com/pg/verify

2.4 Capture

A capture message is used to capture a previously authorized transaction using the payment gateway identifier returned by the authorization message. A capture may

be completed for any amount up to the authorized amount.

URL: https://api.qualpay.com/pg/capture/*<pg_id>*

2.5 Sale

A sale message is used to perform the function of an authorization and a capture in a single message. This message is used in retail and card not present environments where no physical goods are being shipped.

URL: https://api.qualpay.com/pg/sale

2.6 Void

A void message is used to void a previously authorized transaction. Authorizations can be voided at any time. Captured transactions can be voided until the batch is closed. The batch close time is configurable and by default is 11 PM Eastern Time.

URL: https://api.qualpay.com/pg/void/*<pg_id>*

2.7 Refund

A refund message is used to issue a partial or full refund of a previously captured transaction using the payment gateway identifier. Multiple refunds are allowed per captured transaction provided that the sum of all refunds does not exceed the original captured transaction amount.

Authorizations that have not been captured are not eligible for refund.

URL: https://api.qualpay.com/pg/refund/*<pg_id>*

2.8 Credit

A credit message is used to issue a non-referenced credit to a cardholder. A non-referenced credit requires the cardholder data be provided in the message. The credit message is enabled during the first 30 days of production activity.

After 30 days, the credit message is disabled to prevent fraudulent use of the message. If a credit is necessary after 30 days, it is recommended that the merchant make use of the Qualpay web based business platform to issue the credit. If the merchant requires non-referenced credits to be enabled on the payment gateway beyond 30 days they can request this by contacting Qualpay.

URL: https://api.qualpay.com/pg/credit

2.9 Force

A force message is used to force a declined transaction into the system. This would occur when the online authorization was declined and the merchant received an authorization from a voice or automated response (ARU) system. The required fields are the same as a sale or authorization message with the following exceptions: the cardholder expiration date (*exp_date*) is not required, and the 6-character authorization code received from the issuer (*auth_code*) is required.

URL: https://api.qualpay.com/pg/force

2.10　Tokenization

A tokenization message is used to securely store cardholder data on the Qualpay system. Once stored, a unique card identifier is returned for use in future transactions. Optionally, tokenization can be requested in an authorization, verification or sale message by sending the tokenize field set to "true".

URL: https://api.qualpay.com/pg/tokenize

2.11　Batch Close

A batch close message will cause the open batch of transactions to be immediately closed. This message is normally used by POS devices that wish to control the timing of the batch close rather than relying on the daily automatic batch close.

URL: https://api.qualpay.com/pg/batchClose

3. REQUEST AND RESPONSE FIELD DEFINITIONS

3.1 Overview

This chapter provides the field names and descriptions for request (from merchant) and response (to merchant) fields.

3.2 Request Fields

Field Name	Description
merchant_id	Mandatory*, variable length, up to 12 N
	This field identifies the merchant on the acquiring system.
	* CORS requests do not require the *merchant_id*. See the chapter on CORS Support for more information.
security_key	Mandatory*, fixed length, 32 AN
	This field combined with the *merchant_id* authenticates the message.
	* CORS requests do not require the *security_key*. See the chapter on CORS Support for more information.
loc_id	Conditional, variable length, up to 4 N
	When a merchant has more than one location using the same currency, this value is used to identify the specific location. By default this value will be 0.
card_number	Conditional, variable length, up to 19 N
	If present, the field *exp_date* must usually be present and the *card_id* and *card_swipe* fields must not be present.
exp_date	Conditional, fixed length, 4 N, MMYY format
	Required when the *card_number* is present and the message requires an authorization from the card issuer. When the *card_id* is present in the request this field may also be present. If the *card_id* is present and the *exp_date* is not present, then the expiration date from the card vault will be used.
card_id	Conditional, fixed length, 32 AN
	This field contains the *card_id* value received from a tokenization request. The *card_id* may be used in place of a card number in messages requiring cardholder account data.

card_swipe	Conditional, variable length, up to 79 AN
	This field contains either track 1 or track 2 magnetic swipe data. The field sentinels and LRC may be included or omitted from the message. If the magnetic stripe reader (MSR) provides both track 1 and track 2 data in a single read, it is the responsibility of the merchant software to send data for only one of the two tracks.
cardholder_name	Optional, variable length, up to 26 AN
	When provided in a tokenize message, the cardholder name will be stored in the card vault.
cvv2	Conditional, variable length, up to 4 N
	This field contains the CVV2 or CID value from the signature panel on the back of the credit card. If present during a request that requires authorization, the value will be sent to the issuer for validation.
amt_tran	Conditional, variable length, up to 12 N + decimal point
	The total amount of the transaction including sales tax (if applicable). The value can include or omit the decimal section.
	Example $10.00 can be sent as "10" or "10.00".
amt_tax	Optional, variable length, up to 9 N + decimal point
	The amount of sales tax included in the transaction.
partial_auth	Optional
	This field must be present and set to a value of "true" in order for the request to allow for approval of a partial amount. This would be used to allow a merchant to accept a partial payment from a pre-paid gift card.
purchase_id	Optional, variable length, up to 25 AN
	The purchase identifier (also referred to as the invoice number) generated by the merchant.
merch_ref_num	Optional, variable length, up to 128 AN
	This field contains a merchant provided reference value that will be stored with the transaction data and will be included with the transaction data in the Qualpay online reports. This value will also be attached to any lifecycle transactions (e.g. retrieval requests and chargebacks) that may occur.
avs_zip	Optional, variable length, up to 9 N
	The zip code of the cardholder. If present, it will be included in the authorization message sent to the issuing bank.

avs_address	Optional, variable length, up to 20 AN
	The street address of the cardholder. If present, it will be included in the authorization message sent to the issuing bank.
tran_currency	Optional (defaults to 840), fixed length, 3 N
	This field contains the ISO numeric currency code for the transaction.
dba_name	Optional, variable length, up to 25 AN
	When the merchant has been authorized to send dynamic DBA information, this field will contain the DBA name used in the authorization and clearing messages.
	Note, the payment gateway will add a prefix plus an asterisk ('*') to the *dba_name* value. For example, if the prefix is ABC and the *dba_name* value is SHOE CO, the DBA name would be "ABC*SHOE CO". Prefixes can be 3, 7 or 10 characters.
merch_city_ph	Optional, variable length, up to 13 AN
	When the merchant has been authorized to send dynamic DBA information, this field will contain the city or phone data used in the authorization and clearing messages.
merch_phone_cs	Optional, variable length, up to 10 N
	When the merchant has been authorized to send dynamic DBA information, this field will contain the customer service phone number used in the clearing message.
merch_zip	Optional, variable length, up to 10 N
	When the merchant has been authorized to send dynamic DBA information, this field will contain the zip code used in the authorization and clearing messages.
moto_ecomm_ind	Optional (defaults to cardholder present), fixed length, 1 AN
	Possible values: 1 = One Time MOTO transaction 2 = Recurring 3 = Installment 5 = Full 3D-Secure transaction 6 = Merchant 3D-Secure transaction 7 = e-Commerce Channel Encrypted (SSL)
auth_code	Conditional, fixed length, 6 AN
	This field is required when the merchant is sending a force message to the payment gateway. The value of this field should be the 6-character authorization code that the merchant received during a voice or ARU authorization.

line_items	Optional, variable length
	This field is a JSON array of JSON objects. Each object in the array represents a single line item detail element.
	Each detail element is made up of the following subfields.
	Required subfields: *quantity* (7 N): The count of items *description* (26 AN): The description of the item *unit_of_measure* (12 AN): The unit of measure (e.g. inches) *product_code* (12 AN): The product code or SKU number. *debit_credit_ind* (1 AN): D = debit (sold), C = credit (refunded) *unit_cost* (12,2 N) : Cost per unit, up to 2 decimal places
	Optional subfields: *type_of_supply* (2 AN): The type of supply, Visa only *commodity_code* (12 AN): Code used to categorize purchased item, Visa only
	Below is an example of line item detail for a transaction with a total amount of 29.99. ```\n[\n {\n "quantity": "1",\n "description": "Traffic Cones",\n "unit_of_measure": "each",\n "product_code": "SKU-123",\n "debit_credit_ind": "D",\n "unit_cost": "14.99"\n },\n {\n "quantity": "3",\n "description":"Spray Paint",\n "unit_of_measure": "EA",\n "product_code": "SKU-456",\n "debit_credit_ind": "D",\n "unit_cost": "5.00"\n }\n]\n```
pg_id	Conditional, fixed length, 32 AN
	Required when sending a capture, refund or void message type. This value identifies the original transaction that the message should reference during processing.

tokenize	Optional, variable length
	In an authorization, credit, force, sale or verify message the merchant can set *tokenize* to "true" and the payment gateway will store the cardholder data in the vault and provide a *card_id* in the response message if the transaction is approved. If the *card_number* or *card_id* in the request is already in the vault, this flag instructs the payment gateway to update the associated data (e.g. *avs_address*, *avs_zip, exp_date*) if present.
echo_fields	Optional, variable length
	This field contains a JSON array of field data that will be echoed back in the response message.
	Example:
	[{"customer_name": "Joe Smith"},{"customer_id": "123456"}]
retry_id	Optional, variable length, up to 15 N
	This field contains a merchant generated number used to identify the request. This value must be unique within the last 24 hours. When present, the payment gateway will use the *retry_attempt* to determine whether the message is new or a retry of a previous message.
retry_attempt	Conditional, variable length, up to 4 N
	This field contains a positive number greater than zero (0). When the value is one (1), the payment gateway treats the message as a new message. If the value is greater than one (1), then the payment gateway will return the result of the original message. If the original message did not complete, the payment gateway treats the message as a new message. This field is required when the *retry_id* is present in the request message.

3.3 Response Fields

Field Name	Description
pg_id	*Mandatory, fixed length, 32 AN* *This field is a unique identifier generated by the payment gateway and is returned in all valid responses. It should be stored as a reference to the transaction and is required to capture, refund or void a previous transaction.*
rcode	Mandatory, variable length, up to 6 AN This field contains the response code from the payment gateway application.
rmsg	Mandatory, variable length This field contains the response message text from the payment gateway application.
card_id	Conditional, fixed length, 32 AN This field is returned by the tokenize message or when an authorization or sale message requests tokenization of the cardholder data.
auth_code	Conditional, fixed length, 6 AN This field is returned when the message was sent to the card issuer for approval.
auth_avs_result	Conditional, fixed length, 1 AN If the *avs_zip* or *avs_address* is provided in the request message, then the result from the card issuer will be returned in this field.
auth_cvv2_result	Conditional, fixed length, 1 AN If the *cvv2* is provided in the request message, then the result from the card issuer will be returned in this field.
echo_fields	Conditional, variable length If *echo_fields* is present in the request message, then the field will be returned in the response message unmodified.
amt_tran	Conditional, variable length, up to 12 N + decimal point This field is returned on partial approvals.

4. RETRY

4.1 Overview

The payment gateway has support for retrying messages when the merchant application does not receive a response from the Qualpay host. When using retry, the merchant application is responsible for properly handling the *retry_attempt* value.

4.2 Usage

In order to implement the retry, the merchant application should send a number that is unique within the last 24 hours in the request field *retry_id* and a positive number greater than zero (0) in the *retry_attempt* field. For new messages, the *retry_attempt* should be set to a value of one (1). If the merchant application fails to receive a response from the payment gateway, the *retry_attempt* value should be incremented by one (1) and the message should be resent.

When the payment gateway receives a *retry_attempt* value greater than one (1), it will look for a previous message with the same *retry_id* in the last 24 hours. If a previous message is found, the payment gateway will return the response to the previous message. If no previous message is found, the payment gateway will process the message as though it was a new message.

5. CORS SUPPORT

5.1 Overview

Merchant applications can avoid receiving cardholder data by implementing a Cross-Origin Resource Sharing (CORS) tokenize request to the payment gateway to receive a single use *card_id*. This *card_id* can be posted to the merchant site and used in a subsequent payment gateway request. The *card_id* value will remain valid for 10 minutes after the CORS request has been processed. Once the merchant has used the *card_id* in a request to the payment gateway, the *card_id* is no longer valid. The merchant can request that the *card_id* be made permanent by setting the *tokenize* request field to a value of "true" when using the *card_id* for the first time.

5.2 Usage

In order to implement the CORS tokenize request, the merchant checkout process must post a tokenize request from the cardholder's browser directly to the tokenize URL on the payment gateway. The gateway will detect that the request is a CORS request by validating that the x-requested-with HTTP header has a value of XMLHttpRequest. The payment gateway does not require the *merchant_id* or the *security_key* to be included in this type of request.

6. GATEWAY RESPONSE

6.1 Overview

The payment gateway will provide an HTTP status code of 200 (OK) when the request is successful. Unsuccessful requests will receive a non-200 HTTP status code. A more detailed description will be provided in the *rcode* and *rmsg* fields of the response message.

6.2 HTTP Status Codes

Code	Description
200	OK Request was successfully processed by the gateway.
400	Bad Request The request message could not be validated. Refer to the *rcode* and *rmsg* in the response message for more details.
401	Unauthorized The credentials provided were not recognized by the gateway.
402	Declined The request was authorized and validated, but the response from the card issuer was a decline. The field *rmsg* will contain "0" plus the two-character authorization response code.
409	Conflict The request failed due to the state of the transaction. For example, attempts to void a settled transaction would result in a conflict.
500	Internal Server Error The request should be retried.
504	Timeout The authorization request timed out while waiting for the card issuer to respond.

6.3 Gateway Response Codes

Code	Description
000	Success For authorization and sale messages this indicates that the transaction was approved by the card authorization system.
100	Bad request The message was invalid. The field *rmsg* will contain detail about the invalid or missing fields(s).
101	Invalid credentials The *merchant_id* and *security_key* provided do not match the on-file values for the merchant.
102	Invalid *pg_id* The *pg_id* value could not be linked to a valid transaction.
103	Missing cardholder data The request was missing valid cardholder data. Requests requiring cardholder data need only one of the following combinations: *card_number, exp_date* *card_number* (only allowed for force, credit and tokenize messages) *card_id* *card_id, exp_date* *card_swipe*
104	Invalid transaction amount The request was either missing the *amt_tran* or the value provided was invalid. Verify requests require the *amt_tran* to be zero or not present in the request message. Other messages require the *amt_tran* field to be numeric and greater than zero. Negative amounts are not valid.
105	Missing *auth_code* Force transactions require the field *auth_code* in the request message.
106	Invalid AVS data If the field *avs_address* is provided in the request message, then the message must also contain the *avs_zip* field.
107	Invalid expiration date The *exp_date* provided in the request was not properly formatted.
108	Invalid card number The *card_number* field in the request message was non-numeric or contained either too few or too many digits.

109	Field length validation failed
	This *rcode* is returned when any field exceeds the maximum allowed length. The *rmsg* field will contain the name of the first field that failed validation.
110	Dynamic DBA not allowed
	This *rcode* is returned when the request message contained any of the dynamic DBA fields and the merchant has not been approved for dynamic DBA.
111	Credits not allowed
	This *rcode* is returned when an unreferenced credit is submitted and the merchant is not authorized to process credits. Merchants are strongly encouraged to not allow credits to be submitted to the payment gateway.
401	Void failed
	This *rcode* is returned if the transaction has already been captured or voided.
402	Refund failed
	This *rcode* is returned if the transaction has already been refunded, the original transaction has not been captured, the total amount of all refunds exceeds the original transaction amount or the original transaction was not a sale.
403	Capture failed
	This *rcode* is returned if the amount exceeds the authorized amount (except when the merchant category code allows tips), the transaction has already been captured or the authorization has been voided.
404	Batch close failed
405	Tokenization failed
998	Timeout
	This *rcode* is returned if the authorization request timed out without returning a response. Timeouts occur when the authorization system does not receive a response from the host within 10 seconds.
999	Internal error
	This *rcode* is returned when the payment gateway application encountered an unexpected error while processing the request.

7. RESPONSE AND RESULT CODES

7.1 Overview

This section provides the result codes and meanings for the enhanced authorization results.

7.2 AVS Result Codes

Code	Response Text	Description
X	Match	Street address and 9-digit ZIP code both match
Y	Match	Street address and 5-digit ZIP code both match
A	Partial Match	Street address matches, but both 5-digit and 9- digit ZIP Code do not match
W	Partial Match	Street address does not match, but 9-digit ZIP code matches
Z	Partial Match	Street address does not match, but 5-digit ZIP code matches
N	No Match	Street address, 5-digit ZIP code, and 9-digit ZIP code all do not match
U	System Unavailable	Address information unavailable. Returned if non- US. AVS is not available or if the AVS in a U.S. bank is not functioning properly.
R	System Unavailable	Retry - Issuer's System Unavailable or Timed Out.
E	Invalid	AVS data is invalid
S	Not Supported	U.S. issuing bank does not support AVS
D	Match	Street Address and Postal Code match for International Transaction
M	Match	Street Address and Postal Code match for International Transaction
B	Partial Match	Street Address Match for International Transaction. Postal Code not verified due to incompatible formats
P	Partial Match	Postal Codes match for International Transaction but street address not verified due to incompatible formats
C	No Match	Street Address and Postal Code not verified for International Transaction due to incompatible formats
I	No Match	Address Information not verified by International issuer
G	Not Supported	Non-US Issuer does not participate

7.3 CVV2 Result Codes

Code	Description
M	CVV2 Match
N	CVV2 No Match
P	Not Processed
S	Issuer indicates that CVV2 data should be present on the card, but the merchant has indicated data is not present on the card
U	Issuer has not certified for CVV2 or Issuer has not provided Visa with the CVV2 encryption keys

7.4 Card Authorization Responses

7.4.1 Overview

For authorization, sale and verify messages, the *rcode* field in the response message is comprised of three characters and begins with a zero (0). The last two characters will be the response code returned by the authorization system. The table below provides the full description of the authorization system response codes.

7.4.2 Authorization Response Codes

Code	Response Text	Description
00	Approved	Approved and completed successfully
01	Refer to issuer	Refer to card issuer
02	Refer to issuer	Refer to card issuer, special condition
03	Invalid merchant	Invalid merchant
04	Pick up card	Pick up card (no fraud)
05	Decline	Do not honor
06	Error	Error
07	Pick up card fraud	Pick up card, special condition (fraud account)
08	Honor with ID	Honor with ID
10	Partial Approval	Partial approval
11	Approved VIP	Approved (V.I.P)
12	Invalid transaction	Invalid transaction
13	Invalid amount	Invalid amount or currency conversion field overflow

34	Fraud reversal	Used for MasterCard reversal requests only, Suspect Fraud, indicating an approved e-Commerce transaction is cancelled by the merchant
14	Bad card number	Invalid account number (no such number)
15	No such issuer	No such issuer
19	Re-enter	Re-enter transaction
21	No action taken	No action taken
25	Unable to locate	Unable to locate record in file
28	File temporarily unavailable	File temporarily not available for update or inquiry
39	No credit account	No credit account
30	Format error	Format Error - Decline (MasterCard, Discover and PayPal)
32	Partial reversal	Valid for MasterCard Reversal Requests Only - Used in a reversal message to indicate that the reversal request is for an amount that is less than the original transaction.
41	Pick up - Lost	Lost card, pick up (fraud account)
43	Pick up - Stolen	Stolen card, pick up (fraud account)
51	Insufficient funds	Not sufficient funds
52	No checking account	No checking account
53	No savings account	No savings account
54	Expired card	Expired card or expiration date is missing
55	Invalid PIN	Incorrect PIN or PIN missing
57	Not permitted	Transaction not permitted to cardholder
59	Suspected fraud	Suspected fraud
61	Exceeds amount limit	Exceeds approval amount limit
62	Restricted card	Restricted card (card invalid in this region or country)
58	Not allowed at terminal	Transaction not allowed at terminal
63	Security violation	Security violation (source is not correct issuer)
64	AML requirement not fulfilled	Transaction does not fulfill AML requirement
68	Reversal	Used in MasterCard Reversal Requests and Discover and PayPal Responses
65	Activity limit exceeded	Exceeds withdrawal frequency limit
75	PIN entry attempts exceeded	Allowable number of PIN entry tries exceeded

78	Decline	Invalid/nonexistent account - Decline (MasterCard specific)
76	RRN not found	Reversal: Unable to locate previous message (no match on Retrieval Reference number)
77	Invalid reversal data	Previous message located for a repeat or reversal, but repeat or reversal data are inconsistent with original message
79	Already reversed	Already reversed (by Switch)
80	No financial impact	No financial impact (Reversal for declined debit)
81	PIN cryptographic error	Cryptographic error found in PIN
82	Incorrect CVV	Negative CAM, dCVV, iCVV, or CVV results
83	Unable to verify PIN	Unable to verify PIN
84	Decline	Invalid Authorization Life Cycle - Decline (MasterCard) Duplicate Transaction Detected (Visa)
85	No reason to decline	No reason to decline a request for address verification, CVV2 verification, or a credit voucher or merchandise return
86	Cannot verify PIN	Cannot verify PIN; for example, no PVV
89	Ineligible	Ineligible to receive financial position information (GIV)
91	Issuer unavailable	Issuer or switch inoperative and STIP not applicable or not available for this transaction; Time-out when no stand-in; POS Check Service: Destination unavailable; Credit Voucher and Merchandise Return Authorizations: V.I.P. sent the transaction to the issuer, but the issuer was unavailable.
92	Destination not found	Financial institution or intermediate network facility cannot be found for routing (receiving institution ID is invalid)
93	Transaction cannot complete	Transaction cannot be completed - violation of law
94	Duplicate transmission	Duplicate Transmission Detected (Integrated Debit and MasterCard)
96	System malfunction	System malfunction
B1	Surcharge not permitted	Surcharge amount not permitted on Visa cards or EBT food stamps (U.S. acquirers only)
B2	Surcharge not supported	Surcharge amount not supported by debit network issuer
N0	Force STIP	Force STIP
N3	Not available	Cash service not available

N4	Exceeds issuer limit	Cash request exceeds issuer or approved limit
N5	Ineligible for resubmission	Ineligible for resubmission
N7	Decline CVV2 failure	Decline for CVV2 failure
N8	Preauthorized amount exceeded	Transaction amount exceeds preauthorized approval amount
Y3	Offline approved	Unable to go online; offline-approved
Q1	Card authentication failed	Card Authentication failed
Z1	Offline declined	Offline-declined
Z3	Offline-declined	Unable to go online; offline-declined
Y1	Offline approved	Offline-approved
R3	Revocation of authorization	Revocation of All Authorizations Order
T0	First time check	First time check
T1	Check valid - not converted	Check is OK but cannot be converted
T3	Amount exceeds service limit	Amount greater than established service limit
T4	Unpaid items	Unpaid items, failed negative file check
T5	Duplicate check number	Duplicate check number
T6	MICR error	MICR error
T7	Check limit exceeded	Too many checks (over merchant or bank limit)
R0	Stop payment order	The transaction was declined or returned because the cardholder requested that payment of a specific recurring or installment payment transaction be stopped.
R1	Revocation of authorization	The transaction was declined or returned because the cardholder has requested that payment of all recurring or installment payment transactions for a specific merchant account be stopped.
XA	Forward to issuer	Forward to issuer
XD	Forward to issuer	Forward to issuer
R2	Transaction not qualified	The transaction does not qualify for Visa PIN
T2	Invalid transit routing	Invalid Routing Transit Number or check belongs to a category that is not eligible for conversion; Transaction failed ABA check digit validation.

8. Testing

8.1 Overview

This section provides field values for use while testing. Some values will result in known responses to allow developers to test handling of various response codes.

8.2 Test Card Numbers

Card Type	Test Card Number
Visa	4111 1111 1111 1111
MasterCard	5555 5555 5555 4444
Discover	6011 1111 1111 1117
American Express	3714 4963 5392 376
International Diners	3855 5565 0100 05
JCB	3530 1420 1995 5809

8.3 Test Amounts

The table below contains amounts that will cause various *rcode* and *rmsg* values to be returned by the payment gateway.

Test Amount	Response rcode	Response rmsg
0.05	005	Decline
0.10	010	Partial Approval

8.4 Test AVS Data

If the *avs_address* is of the form "123 Main St" followed by "Apt X" then the value of X will be returned as the *auth_avs_result* (even if the value is not a valid AVS result code); this is case insensitive and other characters are allowed, so "st.," and "ST." and "St," all behave in the same way.

For all other inputs, one of six possible responses (based on the length of the data in the two fields) will be returned:

- *avs_zip* can be length 5 (5 match) or 9 (9 match) or other (no match)

- *avs_address* can be length 1-20 (match) or 0 (no match).

8.5 Test CVV2 Data

The table below contains values for the *cvv2* field that can be used to generate various CVV2 result codes in the response message.

CVV2 Value	Response Code
111	M
112	N
113	P
114	S
115	U

9. COUNTRY AND CURRENCY CODES

9.1 Overview

This chapter contains the valid country and currency codes supported by the Qualpay payment gateway. The codes are listed in alphabetical order by the name of the country.

9.2 Supported Countries

ISO Country Name	ISO Alpha Country Code	ISO Numeric Country Code	ISO Numeric Currency Code
Afghanistan	AF	004	971
Albania	AL	008	008
Algeria	DZ	012	012
American Samoa	AS	016	840
Andorra	AD	020	978
Angola	AO	024	973
Anguilla	AI	660	951
Antarctica	AQ	010	578
Antigua and Barbuda	AG	028	951
Argentina	AR	032	032
Armenia	AM	051	051
Aruba	AW	533	533
Australia	AU	036	036

Austria	AT	040	978
Azerbaijan Manat	AZ	031	945
Bahamas	BS	044	044
Bahrain	BH	048	048
Bangladesh	BD	050	050
Barbados	BB	052	052
Belarus	BY	112	974
Belgium	BE	056	978
Belize	BZ	084	084
Benin	BJ	204	952
Bermuda	BM	060	060
Bhutan	BT	064	064
Bolivia, Plurinational State of	BO	068	068
Bonaire, St. Eusatius and Saba	BQ	535	840
Bosnia and Herzegovina	BA	070	977
Botswana	BW	072	072
Bouvet Is.	BV	074	578
Brazil	BR	076	986
British Indian Ocean Territory	IO	086	840
British Virgin Is.	VG	092	840
Brunei Darussalam	BN	096	096
Bulgaria	BG	100	975
Burkina Faso	BF	854	952
Burundi	BI	108	108
Cambodia	KH	116	116
Cameroon, United Republic of	CM	120	950
Canada	CA	124	124
Cape Verde Is.	CV	132	132
Cayman Is.	KY	136	136
Central African Republic	CF	140	950
Chad	TD	148	950
Chile	CL	152	152
China	CN	156	156

Christmas Is.	CX	162	036
Cocos (Keeling) Is.	CC	166	036
Colombia	CO	170	170
Comoros	KM	174	174
Congo	CG	178	950
Cook Is.	CK	184	554
Costa Rica	CR	188	188
Cote D'Ivorie (Ivory Coast)	CI	384	952
Croatia	HR	191	191
Cuba	CU	192	192
Curacao	CW	531	532
Cyprus	CY	196	978
Czech Republic	CZ	203	203
Democratic Republic of the Congo (Zaire)	CD	180	976
Denmark	DK	208	208
Djibouti	DJ	262	262
Dominica	DM	212	951
Dominican Rep.	DO	214	214
Timor-Leste	TL	626	840
Ecuador	EC	218	218
Egypt	EG	818	818
El Salvador	SV	222	222
Equatorial Guinea	GQ	226	950
Eritrea	ER	232	232
Estonia	EE	233	798
Ethiopia	ET	231	230
European Union	N/A	N/A	978
Faeroe Is.	FO	234	208
Falkland Is. (Malvinas)	FK	238	238
Fiji	FJ	242	242
Finland	FI	246	978
France	FR	250	978
France, Metropolitan	FX	249	978

French Guiana	GF	254	978
French Polynesia	PF	258	953
French Southern Territory	TF	260	978
Gabon	GA	266	950
Gambia	GM	270	270
Georgia	GE	268	981
Germany	DE	276	978
Ghana	GH	288	936
Gibraltar	GI	292	292
Greece	GR	300	978
Greenland	GL	304	208
Grenada	GD	308	951
Guadeloupe	GP	312	978
Guam	GU	316	840
Guatemala	GT	320	320
Guinea	GN	324	324
Guinea-Bissau	GW	624	624
Guyana	GY	328	328
Haiti	HT	332	332
Heard and McDonald Is.	HM	334	036
Honduras	HN	340	340
Hong Kong, China	HK	344	344
Hungary	HU	348	348
Iceland	IS	352	352
India	IN	356	356
Indonesia	ID	360	360
Iran, Islamic Republic of	IR	364	364
Iran Airlines	N/A	N/A	365
Iraq	IQ	368	368
Ireland, Republic of	IE	372	978
Israel	IL	376	376
Italy	IT	380	978
Jamaica	JM	388	388

Japan	JP	392	392
Jordan	JO	400	400
Kazakhstan	KZ	398	398
Kenya	KE	404	404
Kiribati	KI	296	036
Korea, Democratic People's Republic of (North Korea)	KP	408	408
Korea, Republic of	KR	410	410
Kosovo, United Nations Interim Administration Mission	QZ	900	978
Kuwait	KW	414	414
Kyrgyzstan	KG	417	417
Lao People's Democratic Republic	LA	418	418
Latvia	LV	428	978
Lebanon	LB	422	422
Lesotho	LS	426	426
Liberia	LR	430	430
Libyan Arab Jamahiriya	LY	434	434
Liechtenstein	LI	438	756
Lithuania	LT	440	440
Luxembourg	LU	442	978
Macao	MO	446	446
Macedonia, the Former Yugoslav Republic of	MK	807	807
Madagascar	MG	450	969
Malawi	MW	454	454
Malaysia	MY	458	458
Maldives	MV	462	462
Mali	ML	466	952
Malta	MT	470	978
Marshall Islands	MH	584	840
Martinique	MQ	474	978
Mauritania	MR	478	478
Mauritius	MU	480	480

Mayotte	YT	175	978
Mexico	MX	484	484
Micronesia, Federated States of	FM	583	840
Moldova, Republic of	MD	498	498
Monaco	MC	492	978
Mongolia	MN	496	496
Montserrat	MS	500	951
Morocco	MA	504	504
Mozambique	MZ	508	943
Myanmar	MM	104	104
Namibia	NA	516	516
Nauru	NR	520	036
Nepal	NP	524	524
Netherlands	NL	528	978
Netherlands Antilles	AN	530	532
New Caledonia	NC	540	953
New Zealand	NZ	554	554
Nicaragua	NI	558	558
Niger	NE	562	952
Nigeria	NG	566	566
Niue	NU	570	554
Norfolk Is.	NF	574	036
Northern Mariana Islands	MP	580	840
Norway	NO	578	578
Oman	OM	512	512
Pakistan	PK	586	586
Palestinian Territory, Occupied	PS	275	840
Palau	PW	585	840
Panama	PA	591	590
Papua New Guinea	PG	598	598
Paraguay	PY	600	600
Peru	PE	604	604
Philippines	PH	608	608

Pitcairn	PN	612	554
Poland	PL	616	985
Portugal	PT	620	978
Puerto Rico	PR	630	840
Qatar	QA	634	634
Republic of Montenegro	ME	499	978
Reunion	RE	638	978
Romania	RON	642	946
Russian Federation	RU	643	643
Rwanda	RW	646	646
Saint Helena, Ascension and Tristan DaCunha	SH	654	654
Samoa	WS	882	882
San Marino	SM	674	978
Sao Tome and Principe	ST	678	678
Saudi Arabia	SA	682	682
Senegal	SN	686	952
Serbia	RS	688	941
Seychelles	SC	690	690
Sierra Leone	SL	694	694
Singapore	SG	702	702
Sint Maarten (Dutch)	SX	534	532
Slovak Republic	SK	703	798
Slovenia	SI	705	798
Solomon Is.	SB	090	090
Somalia	SO	706	706
South Africa	ZA	710	710
So. Georgia and So. Sandwich Is.	GS	239	826
Spain	ES	724	978
Sri Lanka	LK	144	144
St. Kitts-Nevis	KN	659	951
St. Lucia	LC	662	951
St. Pierre and Miquelon	PM	666	250

St. Vincent and The Grenadines	VC	670	978
Sudan	SD	736	736
Sudan Airlines	N/A	N/A	737
Suriname (Guilder)	SR	740	740
Suriname (Dollar)	SR	740	968
Svalbard and Jan Mayen Is.	SJ	744	578
Swaziland	SZ	748	748
Sweden	SE	752	752
Switzerland	CH	756	756
Syrian Arab Rep.	SY	760	760
Taiwan	TW	158	901
Tajikistan	TJ	762	972
Tanzania, United Republic of	TZ	834	834
Thailand	TH	764	764
Togo	TG	768	952
Tokelau	TK	772	554
Tonga	TO	776	776
Trinidad and Tobago	TT	780	780
Tunisia	TN	788	788
Turkey	TR	792	949
Turkmenistan	TM	795	934
Turks and Caicos Is.	TC	796	840
Tuvalu	TV	798	036
Uganda	UG	800	800
Ukraine	UA	804	980
United Arab Emirates	AE	784	784
United Kingdom	GB	826	826
United Nations Mission in Kosovo	QZ	900	978
United States	US	840	840
U.S. Minor Outlying Islands	UM	581	840
U.S. Virgin Is.	VI	850	840
Uruguay	UY	858	858
Uzbekistan	UZ	860	860

Vanuatu	VU	548	548
Vatican City (Holy See)	VA	336	978
Venezuela, Bolivarian Republic of	VE	862	937
Vietnam	VN	704	704
Wallis and Futuna Is.	WF	876	953
Western Sahara	EH	732	504
Yemen	YE	887	886
Zambia	ZM	894	967
Zimbabwe	ZW	716	716

10. EXAMPLES

10.1　　　Authorization

POST /pg/auth HTTP/1.1
Content-Type: application/json
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_11
Host: cert.qualpay.com
Accept: application/json
Connection: keep-alive
Content-Length: 18

{"merchant_id":"212000000001",
"security_key":"cbb1051c8c974837a0a2782b223f935c",
"tran_currency":"840", "card_number":"4888888888888887", "amt_tran":"1",
"exp_date":"1220", "purchase_id":"ABC123"}

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 84
Date: Mon, 29 Sep 2014 18:43:47 GMT

{"rcode":"000","rmsg":"Approved T63362",
"pg_id":"8af556ae480811e484b20c4de99f0aaf"}

10.2　　　Capture

POST /pg/capture/52b992ca441611e480a8005056c00008
HTTP/1.1 Content-Type: application/json
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_11
Host: cert.qualpay.com Accept: application/json
Connection: keep-alive Content-Length: 101

{"merchant_id":"212000000001",
"security_key":"cbb1051c8c974837a0a2782b223f935c", "amt_tran":"1.00"}

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 92
Date: Mon, 29 Sep 2014 18:28:14 GMT

{"rcode":"000","rmsg":"Capture request accepted","pg_id":"52b992ca441611e480a8005056c00008"}

10.3 Sale

POST /pg/sale HTTP/1.1
Content-Type: application/json
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_11
Host: cert.qualpay.com
Accept: application/json
Connection: keep-alive Content-Length: 186

{"merchant_id":"212000000001", "security_key":"cbb1051c8c974837a0a2782b223f935c", "tran_currency":"840", "card_number":"4888888888888887", "amt_tran":"1", "exp_date":"1220", "purchase_id":"ABC123"}

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 84
Date: Mon, 29 Sep 2014 18:43:47 GMT

{"rcode":"000","rmsg":"Approved T42926", "pg_id":"daab5fff480811e484b20c4de99f0aaf"}

10.4 Void

POST /pg/void/f0f85062441311e49863005056c00008
HTTP/1.1
Content-Type: application/json
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_11
Host: cert.qualpay.com

Accept: application/json Connection: keep-alive Content-Length: 81

{"merchant_id":"212000000001",
"security_key":"cbb1051c8c974837a0a2782b223f935c"}

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 86
Date: Mon, 29 Sep 2014 18:30:39 GMT

{"rcode":"000","rmsg":"Transaction
voided","pg_id":"f0f85062441311e49863005056c00008"}

10.5   Refund

POST /pg/refund/52b992ca441611e480a8005056c00008
HTTP/1.1
Content-Type: application/json
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_11
Host: cert.qualpay.com
Accept: application/json
Connection: keep-alive
Content-Length: 81

{"merchant_id":"212000000001",
"security_key":"cbb1051c8c974837a0a2782b223f935c"}

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 91
Date: Mon, 29 Sep 2014 18:33:31 GMT

{"rcode":"000","rmsg":"Refund request
accepted","pg_id":"1c5ff91b480711e4ac850c4de99f0aaf"}

10.6   Tokenize

POST /pg/tokenize
HTTP/1.1
Content-Type: application/json
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_11
Host: cert.qualpay.com
Accept: application/json
Connection: keep-alive Content-Length: 153

{"merchant_id":"212000000001",
"security_key":"cbb1051c8c974837a0a2782b223f935c",
"card_number":"4888888888888887", "exp_date":"1220", "avs_zip":"85284"}

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 135
Date: Mon, 29 Sep 2014 18:36:32 GMT

{"rcode":"000","rmsg":"Token request
complete","pg_id":"88a4099c480711e4ac850c4de99f0aaf","card_id":"88b4363 d480711e4ac850c4de99f0aaf"}

10.7   Force

POST /pg/force
HTTP/1.1
Content-Type: application/json
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.8.0_11
Host: cert.qualpay.com
Accept: application/json
Connection: keep-alive
Content-Length: 168

{"merchant_id":"212000000001",
"security_key":"cbb1051c8c974837a0a2782b223f935c",
"tran_currency":"840", "card_number":"4888888888888887",

"amt_tran":"1.23", "auth_code":"123456"}

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/json
Content-Length: 94
Date: Mon, 29 Sep 2014 19:11:20 GMT

{"rcode":"000","rmsg":"Force transaction accepted","pg_id":"65824102480c11e484b20c4de99f0aaf"}