Merchant Card Payment Engine

Gateway Hosted + IMA Integration Guide

Registered in England No: 2081330. VAT Reg. No: 618184140
Pay360 by Capita Gateway Hosted v 3.0

23rd March 2016

Table of Contents

Table of Figures

1 Getting Started

You will receive a welcome pack via email confirming your application has been accepted and that your account is setup and ready for you to begin integration.

The Pay360 by Capita **Merchant Extranet** is a web based back office system that provides detailed information and powerful tools to assist you in managing your Pay360 by Capita account and can be accessed at the following URL: https://secure.metacharge.com/extranet/

Your welcome pack will contain primary login details for your account. Once logged in you can change passwords and setup access for additional users. Please refer to the Merchant Extranet User Guide for more information.

If you have any questions or you require further information, please contact our dedicated **Merchant Helpdesk**. Their contact details and contact options are all available via the Support tab of the Merchant Extranet. Alternatively please call +44 (0)333 313 7161.

2 Payment Process Overview

The payment process starts with an HTML form POST from your website to the **Merchant Card Payment Engine** (MCPE). This is the **Payment Request**. The consumer is then redirected to our secure payment page to enter their card and personal details. If the payment is authorised, a confirmation receipt is displayed on screen and a copy is emailed to the consumer.

By the time that the confirmation receipt is displayed on screen your server will have already been notified* via a background HTTP POST. This POST is called the **Payment Response Notification** (PRN). We also dispatch an email confirmation to you.
**subject to availability of your nominated web server*

3 Payment Request Initiation

You must submit a minimum of the following five fields to initiate a **Payment Request**. Your request must be submitted by HTTP POST to the "Hosted +IMA" MCPE gateway at: https://secure.metacharge.com/mcpe/purser

- **intInstID** (your preferred "Hosted +IMA" installation number, which is obtained via the Merchant Extranet: *Account Management* > *Installations*)
- **fltAmount** (transaction amount)
- **strCurrency** (3 character ISO currency code for the currency you wish to transact in)
- **strCartID** (order number or session by which you can identify a user/transaction)
- **strDesc** (description of the goods/services you are providing as a result of this transaction)

Once you have successfully integrated the **Payment Request** process with your website, you may submit test transactions on the resultant payment page.

To submit a test transaction, please enter the test VISA card number: 1234123412341234. This card number will automatically be authorised provided you include the field **intTestMode** in your Payment Request, set to 1.

An example test transaction request is below:

```
<form action="https://secure.metacharge.com/mcpe/purser" method="post">
<input type="hidden" name="intTestMode" value="1">
<input type="hidden" name="intInstID" value="123456">
<input type="hidden" name="strCartID" value="YourOrderId/userId/987654321">
<input type="hidden" name="fltAmount" value="29.99">
<input type="hidden" name="strCurrency" value="GBP">
<input type="hidden" name="strDesc" value="description of purchase">
<input type="submit" value="Make Payment">
</form>
```

Simply remove **intTestMode** from your POST when you are ready to proceed with accepting real transactions.

Please note that you can refund transactions within the Merchant Extranet using the *Actions* on the *Transaction Detail* screen for any selected Payment Transaction.

You will only be able to accept real transactions once your Merchant Account is issued by our partner bank. You will be notified by email when this is available.

As part of a **Payment Request** there are a number of optional fields that can be submitted, see Figure 1.

Figure 1: Merchant Card Payment Engine (MCPE) "Hosted +IMA" – Payment Request Parameters

Field	Type(Size)	Required?	Notes
intInstID	int(6)	Yes	The unique identifier for the MCPE "Hosted +IMA" installation that will process this payment.
strCartID	char(192)	Yes	Your own unique identifier for this purchase, to identify the purchase at your end.
intAccountID	int(6)		The MCPE unique identifier for the account to receive funds for this purchase. If this field is omitted, or is invalid, a decision is made based on the currency specified in the *strCurrency* field and the value of the *intTestMode* field (if included).
strDesc	char(192)	Yes	Descriptive text for this purchase.
fltAmount	float(8,3)	Yes	A decimal value representing the transaction amount in the currency specified in the *strCurrency* field, using a point (.) as the separator. **Include no other separators, or non-numeric characters**.
fltSchAmount	float(8,3)		For scheduled payments based upon this transaction, the amount associated with each scheduled payment, in the currency specified in the *strCurrency* field, formatted as for the *fltAmount* field.
strSchPeriod	char(4)		For scheduled payments based upon this transaction, the interval between payments, given as *XY* where *X* is a number (1-999) and *Y* is "D" for days, "W" for weeks or "M" for months.
intRecurs	Int(1)		For scheduled payments, indicates if scheduled payments should recur. Values: 0=no, 1=yes.
strCurrency	char(3)	Yes	The 3-letter ISO code for the currency in which this payment is to be made.
intAuthMode	int(1)		A value to indicate the type of authorisation to use. If this field is omitted, auth with capture is assumed. Values: 0=equivalent to field omitted, 1=auth with capture, 2=pre-auth.
intTestMode	int(1)		If included, indicates a test purchase. A VISA card with card number 1234123412341234 should be used on the payment page. Values: 0=equivalent to field omitted (payment is live), 1=all payments are successful, 2=all payments fail. **Banks are not involved in test payments**.
intTimeout	int(2)		A value indicating the session timeout in minutes. **Values will be capped at 60 minutes**.
datFulfillment	char(10)	As Required	A date the order will be fulfilled, in the format DD/MM/YYYY. May be required as advised for Merchants typically selling travel or tickets.
strCardHolder	char(20)		The name of the card holder, as it appears on the card.
strAddress	char(255)		The purchaser's street address.
strCity	char(40)		The purchaser's town/city
strState	char(40)		The purchaser's county/state
strPostcode	char(15)		The purchaser's postcode
strCountry	char(2)		The 2-letter ISO code for the purchaser's country.
strTel	char(50)		The purchaser's telephone number.
strFax	char(50)		The purchaser's fax number.
Field	**Type(Size)**	**Required?**	**Notes**

By default, the minimum and maximum values of individual transactions on your account are as shown below:

Limits	GBP	USD	EUR
Minimum	£1	$1	€1
Maximum	£1,000	$1,500	€1,500

Please contact your account manager to request different limits on your account, subject to approval by our risk team.

3.1 Subscriptions (Repeat Payments)

The **Merchant Card Payment Engine** supports advanced subscription management. For example, you may set up a subscription offering your customers a trial period with a special introductory rate followed by a regular payment each month. The engine manages scheduling and bills customers automatically. It supports up to 3 levels for each subscription. Each level has an associated amount and period.

This functionality is not enabled by default – please contact your account manager if you would like this feature enabled.

To create subscriptions include fltSchAmount*n*, strSchPeriod*n* (where *n* is 1, 2 or 3) and intRecurs in a **Payment Request**.
intRecurs specifies whether the subscription should continue indefinitely, and always applies to the last level specified.

If you would like a subscription to automatically cancel after '*n*' payments, intCancelAfter determines after how many payments the schedule should be cancelled by the engine.

Here are some examples:

Consumer Proposition	POST to MCPE
£1.00 for the first 7 days, £5.00 per month thereafter	fltSchAmount1 = 1.00, strSchPeriod1=7D fltSchAmount2 = 5.00, strSchPeriod2=1M intRecurs=1
£20.00 per week	fltSchAmount1=20.00, strSchPeriod1=1W intRecurs=1
£2.00 for the first 7 days £5.00 for the next 3 weeks £8.00 per month thereafter	fltSchAmount1=2.00, strSchPeriod1=7D fltSchAmount2=5.00, strSchPeriod2=3W fltSchAmount3=8.00, strSchPeriod3=1M intRecurs=1
£3.00 for the first 7 days £5.00 per month thereafter, automatic cancellation after 6 successful payments	fltSchAmount1 = 3.00, strSchPeriod1=7D intRecurs=1, intCancelAfter=6

Please note that these fields are in addition to the standard (mandatory) fields sent to MCPE, however fltSchAmount1 replaces fltAmount. fltSchAmount1 is the initial payment (first level) of the subscription.

The example POST below will create a subscription billed at £30.00 per month:

```
<input type="hidden" name="intInstID" value="123456">
<input type="hidden" name="strCartID" value="YourOrderId/UserId/987654321">
<input type="hidden" name="strCurrency" value="GBP">
<input type="hidden" name="strDesc" value="description of purchase">
<input type="hidden" name="fltSchAmount1" value="30.00">
<input type="hidden" name="strSchPeriod1" value="1M">
<input type="hidden" name="intRecurs" value="1">
```

3.2 Additional Parameters (Pass-Thru Data)

You have the option of sending any additional arbitrary parameters in the payment request POST that you wish MCPE to return back to you. This is called **Pass-Thru Data**. Any field which starts with the characters **'PT_'** will be passed through MCPE and returned to your server in the contents of the **Payment Response Notification**, see section 5.

```
<input type="hidden" name="PT_SessionStartTime" value="01/02/03:04:05:06">
<input type="hidden" name="PT_FavouriteVegetable" value="sprouts">
<input type="hidden" name="PT_Newuser" value="true">
```

4 User Return

Once the consumer has completed a transaction session, either via a successfully authorised transaction – or by exceeding the maximum permitted transaction attempts, we will return them to your website via HTTP POST.

The location we redirect the consumer to is called the **Return URL** and is configured in the Merchant Extranet. Click *Account Management* then *Installations and* select the installation you wish to configure from the pop-up menu, and then set this URL.

This user return POST contains a single field: **strCartID**. You can use this to retrieve the consumer's order or user details.

Please note that additional parameters specified as Pass-Thru Data does not get returned to you via the User Return. It is only used to aid reconciliation of the PRN, see section 5.

By the time that the consumer has returned to your website Return URL, your web server will have already been notified of the outcome of the transaction via the Payment Response Notification, which will include any Pass-Thru Data provided.

5 Payment Response Notification (PRN)

If a transaction is authorised, you will be notified via HTTP POST. This POST will consist of the original **Payment Request** that you submitted, as well as our additional **Payment Response Parameters** shown in Figure 2, overleaf.

The PRN is enabled and configured on a per-installation basis via the Merchant Extranet. Click on *Account Management* and then *Installations*, then select the relevant "Hosted +IMA" installation from the dropdown menu.

In order to receive the PRN, you must first complete the following fields for the appropriate installation:

- **Response URL**: The URL where you want the PRN to be sent, for example http://www.merchant.com/script.name

Where consumers are entered into subscriptions, we will notify you on each occasion that further payment is processed by the engine, or if the subscription fails or is terminated. To receive this you may configure an additional Response URL.

- **Scheduled Payment Response URL**: Configured as above if subscriptions have been enabled on your installation.

We recommend that you perform HTTP Basic Authorisation on your web server to ensure that the response is coming from a trusted source, in this case MCPE. If you have enabled HTTP Basic Authorisation on your server, you will need to specify:

- **Response HTTP Auth Username**
- **Response HTTP Auth Password**

In order for you to get accustomed to and develop software to act upon the Payment Response Notifications, we have created a Notification Test Suite within the Merchant Extranet. The test suite can send example responses to a URL of your choice. Click on the *Resources* tab and then *Notification Suite* on the sub menu to access the test suite.

The range of possible PRN parameters is described in Figure 2, overleaf.

Figure 2: MCPE "Gateway Hosted +IMA" – Payment Response Parameters

Field	Type(Size)	Notes
intTransID	int(11)	The MCPE unique identifier for this transaction.
intScheduleID	int(11)	The MCPE unique identifier for any payment schedule associated with this transaction (if applicable).
intAccountID	Int(11)	The account used for the transaction
intStatus	int(1)	The status of this transaction. Values: 0=failed, 1=successful
intTime	int(11)	The time, at which this transaction was authorised, given as the number of seconds since the start of 1970 GMT. This is omitted in the event of a cancelled transaction.
fltAmount	float(8,3)	The amount associated with this transaction, in the currency specified in the *strCurrency* field.
strCurrency	char(3)	The 3-letter ISO code for the currency associated with this transaction (uppercase).
strMessage	char(255)	Any message returned by the bank when this transaction was processed.
strPaymentType	char(10)	The purchaser's card type. Values: VISA, MC, DELTA, SOLO, SWITCH, UKE.
intAVS	int(1)	The result of the AVS check performed for this transaction. **This field will be omitted if the check was not performed**. Values: 0=AVS check failed, 1=AVS check passed.
intCV2	int(1)	The result of the CV2 check performed for this transaction. **This field will be omitted if the check was not performed**. Values: 0=CV2 check failed, 1=CV2 check passed.
strCustomer	char(100)	The card holder's name.
strAddress	char(100)	The card holder's street address.
strCity	Char(50)	The card holder's city
strState	Char(50)	The card holder's state/county
strPostcode	char(20)	The card holder's postcode.
strCountry	char(2)	The 2 digit ISO code of the consumer's country of origin.
strTel	char(20)	The card holder's telephone number.
strFax	char(20)	The card holder's fax number.
strEmail	char(100)	The card holder's email address.
strDesc	char(100)	The description of the transaction
strCartID	char(192)	The cartID of the transaction
strTransactionType	char(20)	'Payment', 'Repeat Payment, 'Refund', or 'Chargeback'
strSyndicate	char(20)	Will always be 'default'.
fltFraudScore	decimal(2,3)	Likelihood of the transaction being fraudulent. A value between 0.000 and 10.000, 0.000 being the most unlikely and 10.000 being the most likely.
fltNotifyVersion	decimal(1,1)	The version of the notification. Currently this is at 1.5. When we change our API, we will let you know both in an email approximately 2 weeks before the change, and we will increment this number once the new API has gone live.

Figure 3: MCPE "Gateway Hosted +IMA" – Subscription Payment Response Parameters

Field	Type(Size)	Notes
intTransID	int(11)	The MCPE unique identifier for this transaction.
intScheduleID	int(11)	The MCPE unique identifier for the payment schedule associated with this transaction.
intStatus	int(1)	The status of this transaction. Values: 0=failed, 1=successful
intTime	int(11)	The time, at which this transaction occurred, given as the number of seconds since the start of 1970 GMT.
fltAmount	float(8,3)	The amount associated with this transaction, in the currency specified in the *strCurrency* field.
strCurrency	char(3)	The 3-letter ISO code for the currency associated with this transaction (uppercase).
strPaymentType	char(6)	The purchaser's card type. Values: VISA, MC, DELTA, UKE, SOLO, SWITCH, AMEX
intRelatedID	int(11)	The MCPE unique identifier for the initial transaction associated with the subscription specified in *intScheduleID*.
strMessage	char(255)	If the transaction has failed, the reason is given here.

There are two additional response notifications which are sent in the event of subscription cancellation or end of term:

Field	Type(Size)	Notes
intScheduleID	int(11)	The MCPE unique identifier for the payment schedule.
intStatus	int(11)	The status of this subscription. Values: 2=cancelled, 3=end of term

5.1 Example Responses

Figure 4: The Payment Response Notification for a successful one-time transaction

Field	Example Value	Notes
intTransID	123456789	The MCPE unique identifier.
intScheduleID		There is no schedule for this transaction.
intInstID	123456	Your MCPE installation number.
strCartID	YourOrderId/userId/987654321	Your own unique identifier for this purchase, to identify the purchase at your end.
intAccountID	1234	The account used for the transaction.
intTime	1200000000	Time of the transaction, in seconds past 1970.
IntStatus	1	The transaction was successful.
strDesc	Teddy Bear	
fltAmount	15.00	Transaction amount.
strCurrency	GBP	
strMessage		
strPaymentType	SWITCH	A Switch card was used for this purchase.
intTestMode	0	This was a real transaction.
intAVS		There was no AVS check
intCV2	1	The CV2 check was successful.
strCustomer	John Doe	
strAddress	1, Regency Square	
strPostcode	PP1 5DV	
strCountry	UK	
strTel	+44 1234 56778	
strFax		No fax number was given.
strEmail	john@doe.org	

The PRN would look like this:

```
intTransID=123456789&intInstID=123456&strCartID=YourOrderId/userId/987654321&intAccoun
tID=1234&intStatus=1&strDesc=Teddy_Bear&fltAmount=15.00&strCurrency=…etc
```

Figure 5: The Payment Response Notification for an unsuccessful one-time transaction

Field	Example Value	Notes
intTransID	123456789	The MCPE unique identifier.
intScheduleID		There is no schedule (subscription) for this transaction.
intInstID	123456	Your MCPE installation number.
strCartID	YourOrderId/UserId/987654321	Your own unique identifier for this purchase, to identify the purchase at your end.
intAccountID	1234	The account used for the transaction.
intTime	1200000000	Time of the transaction, in seconds past 1970.
intStatus	0	The transaction failed.
strDesc	Teddy Bear	
fltAmount	15.00	Transaction amount.
strCurrency	GBP	
strMessage	The card number given is invalid	The message received from the bank when attempting to process this transaction.
strPaymentType	VISA	A Visa card was used for this purchase.
intTestMode	0	This was a real transaction.
intAVS		There was no AVS check
intCV2		There was no CV2 check
strCustomer	John Doe	
strAddress	1, Regency Square	
strPostcode	PP1 5DV	
strCountry	UK	
strTel	+44 1234 56778	
strFax		No fax number was given.
strEmail	john@doe.org	

Figure 6: The Payment Response Notification for a successful subscription

Field	Example Value	Notes
intTransID	123456789	The MCPE unique identifier.
intScheduleID	10000	The schedule with ID 10000 is associated with this transaction.
intInstID	123456	Your MCPE installation number.
strCartID	YourOrderId/UserId/987654321	Your own unique identifier for this purchase, to identify the purchase at your end.
intAccountID	1234	The account used for the transaction.
intTime	1200000000	Time of the transaction, in seconds past 1970.
intStatus	1	The transaction was successful.
strDesc	Subscription to Bloggs Blog	
strCurrency	GBP	
strMessage		
strPaymentType	MC	A Mastercard was used for this purchase.
fltSchAmount1	1.00	The initial subscription amount
strSchPeriod1	1W	The initial subscription period
fltSchAmount2	5.00	The subsequent subscription amount
strSchPeriod2	1M	How long this amount lasts for
intRecurs	0	This subscription does not recur, so after 1 month we will send an End Of Term notification to you.
intTestMode	0	This was a real transaction.
intAVS		There was no AVS check
intCV2		There was no CV2 check
strCustomer	John Doe	
strAddress	1, Regency Square	
strPostcode	PP1 5DV	
strCountry	UK	
strTel	+44 1234 56778	
strFax		No fax number was given.
strEmail	john@doe.org	

Figure 7: The Payment Response Notification for a successful subscription payment

Field	Example Value	Notes
intTransID	987654321	The MCPE unique identifier for this transaction.
intRelatedID	123456789	The initial transaction associated with this payment subscription (see Figure 6)
intScheduleID	10000	The payment schedule (subscription) identifier.
intTime	1300000000	Time of the transaction, in seconds past 1970.
intStatus	1	The transaction was successful.
fltAmount	3.00	Transaction amount.
strCurrency	GBP	
strFriendly	GBP3.00	
strPaymentType	MC	A MasterCard was used for this purchase.

Figure 8: The Payment Response Notification for a failed subscription payment

Field	Example Value	Notes
intTransID	987654321	The MCPE unique identifier for this transaction.
intRelatedID	123456789	The initial transaction associated with this payment subscription (see Figure 6)
intScheduleID	10000	The payment schedule (subscription) identifier.
intTime	1300000000	Time of the transaction, in seconds past 1970.
intStatus	0	The transaction was unsuccessful.
fltAmount	3.00	Transaction amount.
strCurrency	GBP	
strPaymentType	MC	A MasterCard was used for this purchase.

Figure 9: The Payment Response Notification for an end of termed subscription

Field	Example Value	Notes
intScheduleID	10000	The MCPE unique identifier for the subscription.
intStatus	3	The subscription has end of termed

Figure 10: The Payment Response Notification for a cancelled subscription

Field	Example Value	Notes
intScheduleID	10000	The MCPE unique identifier for the subscription.
intStatus	2	The subscription has been cancelled

6 Payment Page Design

"Hosted +IMA" is our fully hosted secure payment solution. Payment is made via a tried and tested payment page which captures full address and contact details from the consumer.

By default this solution is branded as Pay360 by Capita. We offer the option of re-branding the payment solution to match your web site, through incorporation of a customer header graphic.

To add this custom header graphic, email a 750x100 pixel JPEG or GIF image to completesupport@paypoint.net quoting your intended installation ID. We will install this accordingly.

If you require further control over the payment page or the consumer experience in general, consider upgrading to Freedom + IMA. Please ask your account manager for details.

7 Preventing Online Credit Card Fraud

Pay360 by Capita recommend **FraudGuard**. This real-time fraud service operates on all "Gateway Hosted +IMA" transactions unless otherwise expressly agreed.

Transactions processed via "Hosted +IMA" MCPE with FraudGuard result in detailed transaction information available via the Merchant Extranet. These enable you to make more qualified judgements about each of your consumers.

FraudGuard data includes powerful metrics covering GeoIP location (the actual location of the consumer), card issuer location, and discrepancies therein – plus a vast array of other measures including number of recent similar requests.

The service acts to screen all transactions by generating a FraudGuard score. It also provides detailed Territory Management and a Blacklisting and Whitelisting function.

However, additional techniques can be used with "Hosted +IMA" MCPE to gain further confidence

7.1 Manual Checks

Know Your Customer (KYC)

KYC is a process many businesses use to establish more trusting and hence more profitable relationships with consumers. It can be used to evaluate suspicious consumers or before acceptance and/or fulfilment of higher value transactions.

There is no single process attached to KYC but it would typically involve validating the cardholder identity. This might be achieved by collecting telephone number at payment and contacting the consumer to establish their identity, or any other cross-check.

It might involve querying the issuer of their card and checking that against information published on Transaction Detail via the Merchant Extranet.

Manual Authorisation with Signature

This is an excellent way of verifying the card holder as part of a formal KYC process. It also serves as strong mitigation against the risk of Chargebacks.

This manual authorisation process involves sending a consumer a transaction confirmation document to sign and return with copies of their card. The trade-off is that it makes the customer do more work, but serves as excellent fraud mitigation.

For your convenience, Pay360 by Capita provides a part-completed manual authorisation form via a link on each transaction detail screen on the Merchant Extranet. Simply launch the form from alongside the cardholder name and email/fax to the consumer.

7.2 Automated Processes

Deferred (Pre-Authorised) Transactions

Any **Payment Request** can be submitted as a Pre-Authorisation. This means the card is not debited immediately but instead the transaction can be completed within 7 days, either manually via Merchant Extranet or by setting an automatic delayed capture.

Automated capture is configured for your account via *Account Management* > *Installations*. Deferring transactions gives you the opportunity to evaluate risk before accepting liability. It gives you a risk free period in which to conduct KYC processes.

Number of Attempts

Many additional controls exist in MCPE. To reduce the risk of a fraud attack and to control processing costs, the consumer is permitted a limited number of failed attempts per session. You can set this via Account *Management* > *Installations.*

As well as the minimum and maximum transaction limits which were described at the bottom of page 4, we also control the maximum number of attempts from a unique card or IP within any 24 hour period. Our Risk team can adjust this for you.

8 Frequently Asked Questions (FAQ)

8.1 Where does the PRN come from?

The PRN should originate from one IP address. However since Pay360 by Capita operates a large network infrastructure with multiple fail over capacity, we do not encourage Merchants to expect communications originating from a single IP. Please make sure that your firewall and web servers are configured to allow connections only from the domain metacharge.com. Guidance on fixed IP addresses is available upon request.

8.2 How does Pay360 by Capita determine that a PRN is successfully received?

This is done using HTTP server return codes. In the event that your script responds with anything other than a return code in the range of 200 to 206 we will assume that you did not receive or process the PRN. We will subsequently retry delivery of this PRN at increasing time intervals for a period of up to 24 hours. Should a PRN be undeliverable for 24 hours we can notify you via email.

We will also assume the PRN has failed if your response URL does not return HTTP headers within 2 seconds. At which point we will terminate the client connection. You should note that in this instance some server side scripting languages terminate instantly and so your scripts will not complete. In general this is normally a configuration option in the scripting language or web server environment you are running. We also recommend that you have a procedure in place to check for duplicate PRN's.

8.3 Are HTTP redirects supported?

Yes.

8.4 What protocols are supported?

A Response URL can reside on HTTP or HTTPS domains. We will also post to secure domains that have self signed certificates.

8.5 How can I improve security?

Here are some things you can do to improve security:

- Password protect your Response URL's using HTTP Basic Authorisation and via *Account Management* > *Installations*
- Configure the Response URL to only accept connections from the domain metacharge.com
- Ensure the Response URL is only accessible via HTTPS
- Send a Pass Thru ('PT_') parameter containing a hash of Payment Request values and validate it on receipt of PRN

8.6 How do I update my response URL?

Click on *Account Management* then *Installations* within the Merchant Extranet.