EDT MAKING BEST PRACTICE COMMON PRACTICE

UK Government Gateway

Payment Engine Business Overview

Version:	3.0
Owner:	Jim Purves
Status:	Baseline
Security Classification:	NON-PROTECTIVELY MARKED
Date:	05 July 2006

Revision & Sign-Off Sheet

Change Record

Date	Author	Version	Status	Change Reference
15th Dec 04	Paul Knapton	0.1	Draft	First draft for review
15th Mar 05	Paul Knapton	0.3	Baseline Candidate	Changes following (final) customer review
5th April 05	Filippa Price	1.0	Baseline	Baseline document added to customer documentation set
17th Nov 05	Mark Taylor	2.0	Baseline Candidate	Amended time pre-auth is valid until expires
5th July 06	Mark Taylor	3.0	Baseline	Added Payment AR 1.2 functionality

Document Status has the following meaning:

- **Drafts** – These are documents for review and liable to significant change.
- **Baseline Candidate** – The document is ready for final issuing and is only expected to have further minor updates. This document will have changes tracked since the Working Baseline (In Test).
- **Baseline** – The document is published and is not expected to change. This document will have changes tracked since the Working Baseline.

Note that minor updates or corrections to a document may lead to multiple versions at a particular status.

Reviewers

Name	Version Approved	Position	Date
Jim Purves	3.0	Gateway Product Owner	5th July 06

e-Government Unit, Cabinet Office
Stockley House
130 Wilton Road
London SW1V 1LQ

http://www.cabinetoffice.gov.uk/e-government/

Table of Contents

REVISION & SIGN-OFF SHEET **I**

CHANGE RECORD I
REVIEWERS I

1 INTRODUCTION **1**

1.1 INTENDED READERSHIP 1
1.2 PURPOSE 1
1.3 GLOSSARY OF TERMS AND ABBREVIATIONS 1

2 GOVERNMENT GATEWAY PAYMENT ENGINE - OVERVIEW **2**

2.1 BUSINESS BENEFITS OF USING GGPE 3
2.2 PROCESSING FLOW OVERVIEW – CARD PAYMENTS 4
2.3 PROCESSING FLOW OVERVIEW – DIRECT DEBITS 5

3 SETTING UP A PAYMENT SERVICE **6**

3.1 MERCHANT ID 6
3.2 SERVICE STRUCTURE 6
3.3 CARD TYPES 6
3.4 CURRENCY 6
3.5 PAYMENT AMOUNT LIMITS 6
3.6 SECURE REFUNDS 6
3.7 ORIGINATOR'S IDENTIFICATION NUMBER (DIRECT DEBITS) 6

4 CARD PAYMENT PROCESSING **8**

4.1 CAPTURING THE CARD DETAILS 8
4.2 CV2AVS CHECKING 9
4.2.1 Policy Usage *9*
4.3 CARD DETAIL VALIDATION 9
4.4 DATACASH PROCESSING 10
4.5 PAYMENT ENGINE RESPONSE TO DEPARTMENT WEB SITE 10
4.6 PAYMENT ENGINE RESPONSE TO DEPARTMENT BACK-OFFICE (NON DIS) 11
4.7 PAYMENT ENGINE RESPONSE TO DEPARTMENT BACK-OFFICE (DIS ONLY) 11
4.8 SETTLEMENT OF THE TRANSACTION 11
4.9 TWO-STEP PAYMENT PROCESS 11
4.9.1 Pre-Authorisation *12*
4.9.2 Fulfilment *12*

5 DIRECT DEBITS **13**

5.1 CAPTURING THE DDI SET-UP DETAILS 13
5.2 DDI SET-UP VALIDATION 13
5.3 DATACASH DDI SET-UP PROCESSING 14
5.4 PAYMENT ENGINE RESPONSE TO DEPARTMENT WEB SITE 14
5.5 PAYMENT ENGINE RESPONSE TO DEPARTMENT BACK-OFFICE (NON DIS) 14
5.6 PAYMENT ENGINE RESPONSE TO DEPARTMENT BACK-OFFICE (DIS ONLY) 15
5.7 DRAW DOWNS 15

6 REFUNDS **17**

7 SECURE REFUNDS **18**

8 PAYMENTS HELPDESK APPLICATION FUNCTIONALITY **19**

9 MISCELLANEOUS FUNCTIONALITY **20**

9.1 RECONCILIATION OF BANK TOTALS 20
9.2 TIME OUTS 21
9.3 DUPLICATE PAYMENT CHECKING 21

APPENDIX A - ADDITIONAL INFORMATION **22**

1 Introduction

1.1 Intended Readership

The intended audience of this document is Departments and Local Authorities (LAs) seeking a business focussed overview of the functionality of the Government Gateway Payment Engine and the benefits that can be gained by using it. This is not a technical document. Intended readership would therefore more likely be IT Managers, Heads of IS, Finance Directors or Project Managers looking to understand more fully how the GGPE could support their business requirements.

1.2 Purpose

The purpose of this document is to provide Departments and Local Authorities with a detailed understanding of how the Government Gateway Payment Engine (GGPE) works – but at a business rather than technical level. It describes the core functionality of the GGPE and the end to end process for a Department taking on-line payments using GGPE. Where a level of technical detail is required to further understand the business process it has been included here, but this document is not intended to provide developers with a definitive functional or interface specification; they are available separately if required.

This document is a business overview of the Gateway Payment Engine functionality and designers and developers should refer to the appropriate technical specifications to confirm detailed system processing.

1.3 Glossary of Terms and Abbreviations

Abbreviation	Definition
Customer	A Department, Local Authority or Government Agency using or considering using the Gateway Payment Engine.
CV2AVS	The Address and Security Code Verification Service
DDI	Direct Debit Instruction – the authorisation under the Direct Debit scheme to debit monies from a bank account.
DIS	Department Interface Server
EDT	e-Delivery Team
eGU	e-Government Unit
GGPE	Government Gateway Payment Engine
GSI	Government Secure Intranet – a secure network for use within and between Government Departments
LAs	Local Authorities
PSP	Payment Service Provider – third party managed service for the handling of payment interactions with card providers, banks, BACS etc
SI	System Integrator – EDT supplier used to build new Gateway services.
SSL	Secure Socket Layer – the industry standard mechanism for ensuring encryption of information exchanges over the internet.
UAT	User Acceptance Testing
VM Gateway	New service built onto a ‘Virtual Machine’ deployed to Departments on DVD to provide a simulated Gateway for Departments to develop their front and back ends against..

2 Government Gateway Payment Engine - Overview

The Government Gateway Payment Engine is a pan-Government facility that enables Departments, Local Authorities and Agencies to connect to the Merchant Acquirer of their choice for the collection of on-line payments by debit or credit card. The Payment Engine uses a 3rd Party Payment Service Provider – Datacash - to validate, authorize and collect payments.

Card payments may be made using most debit (Switch, Solo, etc) and credit (VISA, Mastercard, Amex etc) cards, configurable for each Departmental Service. The Payment Engine will support multiple currencies if required. As standard it will support Sterling.

The Payment Engine also accepts CV2AVS fraud checking for card payments. This checking will help to identify and reduce the impact of fraudulent transactions.

The Payment Engine also supports paperless Direct Debit set-up and draw down.

Connection to the Gateway (via a DIS box) provides Departments and Local Authorities with improved back-end business integration and functionality including immediate departmental notification of payments received and the ability to generate a payment or refund directly from the Departments back end systems

Connection to the Gateway (via DIS) is not however mandatory – the Payment Engine can be used as an internet only service, with 128-bit SSL connections to portals.

Reconciliation of payments made is supported by the Departmental Notification process, as well as standard MIS reporting.

Where the Payment Engine is being used via the internet only, reconciliation will be done with the Merchant Acquirer as normal, supported where necessary by payments information captured by the Departmental Portal.

A help desk application is available to Departmental Support Staff. The help desk will enable queries to be made against the payment database to determine the status of a payment request, as well as refunds to be made against a payment, Refunds are also available as a secure facility called ‘Secure Refunds’. This is accessible outside of the help desk application, so batch refunds can be made.

The Payment Engine can be used as a single channel for payments, integrating call centre, telephone (IVR) or kiosk applications through the same engine. Where the Payment Engine is used in this way, consideration will need to be given to the integration of the payment details with the calling channel to ensure that business and accounting requirements (e.g. daily balancing by User) are met.

2.1 Business Benefits of using GGPE

There are a number of business benefits in using the Government Gateway Payment Engine. As well as having access to the full range of features and support provided by one of the market-leading Payment Service Providers (Datacash), the Payment Engine provides an additional layer of functionality and support tailored for Government use.

These include:

- Help Desk Application for supporting payments queries and for making refunds
- Real-time Notifications to back office (via DIS box) of Payments made to ensure customer and/or financial systems are up to date
- Support for fully paperless Direct Debits (Set-Up and Draw Down)
- A proven trusted partner/supplier – and therefore lower risk
- High resilience and availability
- A fully customisable presentation layer to match portal look and feel.

One of the key benefits is that Departments and Local Authorities can take advantage of the pan-Government deal that Cabinet Office have entered into with Datacash whereby transaction charges reduce as pan-Government volumes of transactions through the Payment Engine increase. This enables all Government bodies to benefit regardless of their own volumes.

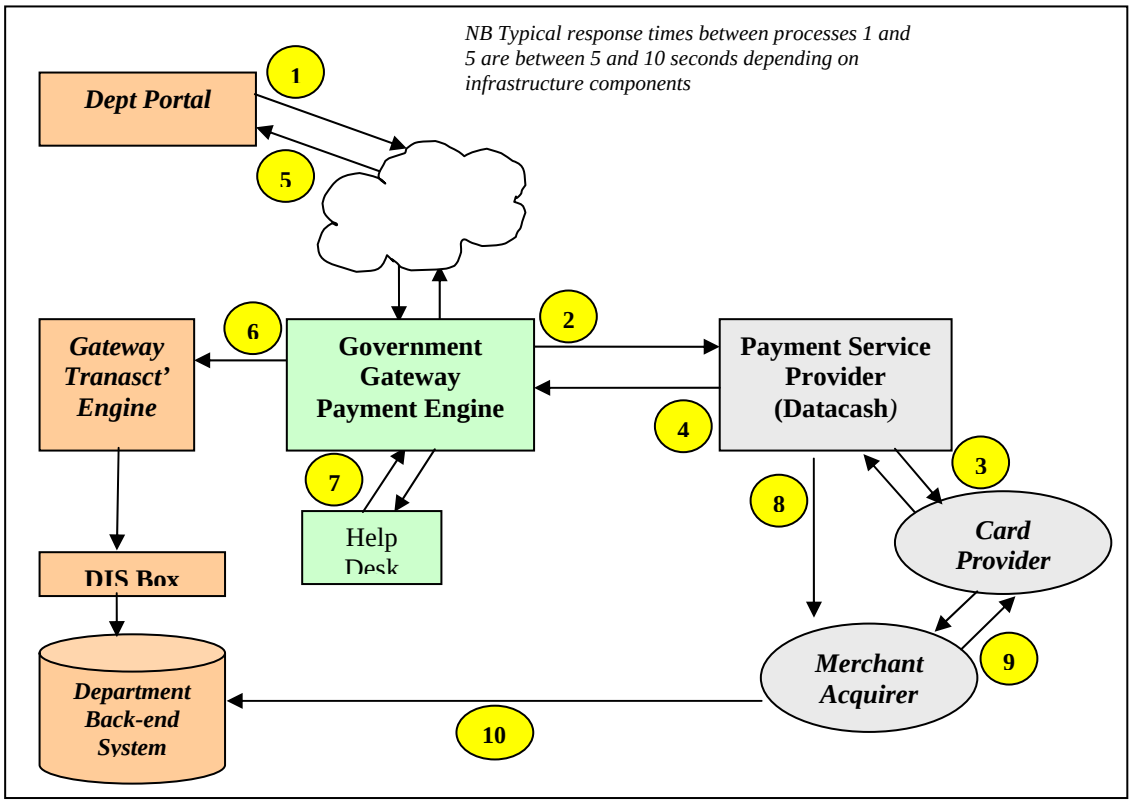
For more details of transaction charges please contact the EDT team within Cabinet Office (edt@cabinet-office.x.gsi.gov.uk)

Because the contract with Datacash is managed through Cabinet Office, the Payment Engine solution (and Datacash service) is pre-procured, saving Departments and LAs a considerable amount of time and effort, not to mention cost, by not having to go through a formal tendering or procurement process.

Additionally, the Payment Engine provides a level of abstraction from the Payment Service Provider for Departments and Local Authorities, protecting them from API changes as far as possible. This means that should an existing PSP fail to continue to provide best value or service then the impact of migration to an alternative PSP can be minimised for Departments or Local Authorities using the Gateway Payment Engine.

Not only does the Gateway Payment Engine represent a low cost entry to re-use of a piece of Common Infrastructure but that investment also provides a key stepping stone to integration of enterprise wide payments services as well as to additional corporate services provide by Gateway such as Authentication and Authorisation (R&E).

2.2 Processing Flow Overview – Card Payments



1. Department website or portal (or IVR) captures payment information from customer and sends Payment Request via the internet to Government Gateway Payment Engine.

2. Payment Engine performs some initial validation of Payment Request before passing Request to Payment Service Provider (Datacash).

3. Datacash requests authorisation from Card Provider (VISA Mastercard etc). Card Provider checks that request is valid (funds available, card valid etc) and passes response back to Datacash.

4. On receipt of response, Datacash stores payment request in batch file for later settlement and passes details of response to Payment Engine.

5. On receipt of response from Datacash, Payment Engine stores payment details and passes response details back to Department web.

6. If DIS box is implemented, Payment Engine also passes Notification to Department Back-End system for updating of Customer or financial record with payment details.

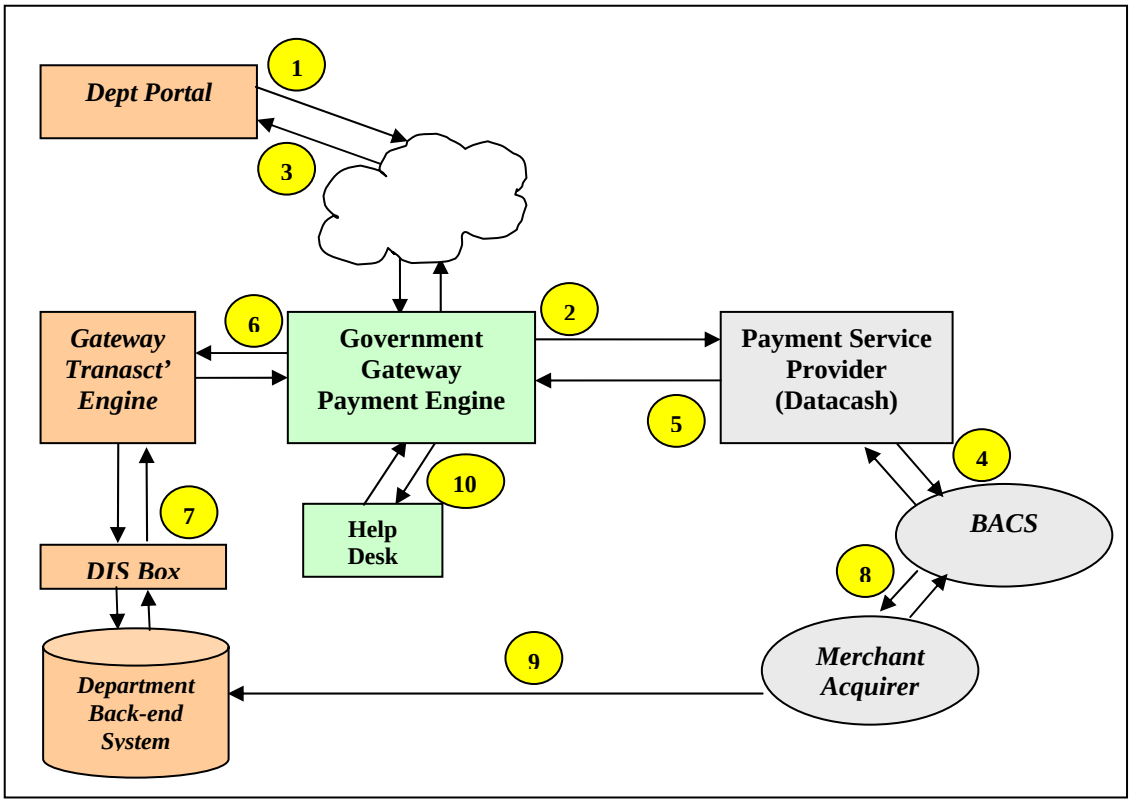
7. Department support staff can use Help Desk application to check status of payment requests and to make refunds against payments made.

8. At the end of each day, Datacash sends the batch of authorised Payment Requests to the Department's Merchant Acquirer (bank) for settlement

9. The Merchant Acquirer request funds from the Card Provider for the authorised Payment Requests. Funds appear in Merchants bank account between one and three days later.

10. Department reconciles bank statement with back-office payment records to account for monies. Additional MIS available from Help Desk and Datacash to reconcile mismatches on amounts.

2.3 Processing Flow Overview – Direct Debits



1. Department website or portal captures Direct Debit Instruction (DDI) information from customer and sends DDI Set-up Request via the internet to Government Gateway Payment Engine.

2. Payment Engine performs some initial validation of DDI Set-up Request before passing Request to Payment Service Provider (Datacash).

3. Datacash checks DDI Set-up request is a valid request and if it is, informs Payment Engine that Set-up Request has been successfully received (but not yet authorised). Payment Engine passes response (in real-time) to calling Department website.

4. Datacash passes Set-up Request to BACS for processing, and under the industry DD Scheme, BACS registers the Set-up request with the relevant Merchant Acquirer (bank) . If approved, BACS informs DataCash that set-up was successful along with a DDI number.

5. Datacash informs Payment Engine that Set-Up was successful, along with the DDI number.

6. Gateway Payment Engine informs Department Back-Office system (via DIS box) that the Set-Up was successful, and includes the DDI number.

7. Departments may request Draw Downs (taking money from the customer account) against an authorised DD Instruction via a Gateway DIS box. Payment Engine will check Draw Down before logging and passing to Datacash who do similar before passing to BACS.

8. BACS request settlement of funds between customers and Departments' banks.

9. Drawn Down amounts will appear on Departments bank statement for reconciliation. Where Draw Downs fail (account closed etc) an additional report (ARRUD) is available from banks.

10. Department staff may check status of DDI Set-up requests and Draw Downs using the Payment Engine Help Desk. They may also make refunds against Draw Downs.

3 Setting up a Payment Service

There are a number of business decisions or actions required as part of the setting up of a Payment Service using the GGPE.

3.1 Merchant ID

The Department or Local Authority is responsible for obtaining an e-commerce Merchant ID (MID) from their bank. This is normally a straightforward process but is essential for taking payments via the internet.

3.2 Service Structure

The Department will determine the Service structure they wish to employ. A Service in this context defines the level at which the payment will be made within the organisation. For example a Local Authority may choose to create a single Service relating to the whole Authority, or may have multiple Services for each payment type (for example one for Council Tax, one for parking fines etc). Where one Service is used, only one MID is required, but it will be the Authorities responsibility to carry sufficient data in the User Transaction Ref fields (see below) to determine what is being paid for. Where multiple services are created, a MID will be required for each Service.

3.3 Card Types

The Payment Engine accepts all of the major UK credit and debit cards:

- VISA
- Switch
- Solo
- Diners Club
- Mastercard
- Maestro
- JCB
- American Express

The card types actually accepted by a Department or Local Authority for a specific Service are configurable on a Service by Service basis – for example not all Departments or LAs will want to accept American Express because of the increased cost.

3.4 Currency

GGPE is a multi currency solution supporting over 70 international currencies for payments. Sterling is supported as standard, and other currencies, including the Euro, are available on request at a small additional cost.

3.5 Payment Amount Limits

Each service has a minimum and maximum payment amount which enables the Department to add an extra level of validation to the card processing to trap any unnecessary errors. For example if a service typically requires a payment of a fee of £100, then to avoid end users accidentally typing in £10 or £1000, the service minimum limit could be set to £15 and the service maximum limit could be set to £999. Any payment request with an amount outside of those limits would be rejected by GGPE.

3.6 Secure Refunds

Each service has the option to assign a username and password for access to Secure Refunds (see 7 below). This will give the department the ability to access and process secure refunds via the web services available through Payment Engine.

3.7 Originator's Identification Number (Direct Debits)

In order to be able to set up paperless Direct Debits, the Department or Authority need to get approval from the Direct Debit Scheme owners (BACS). This approval comes in the form of an Originator's

Identification Number (OIN) which can be obtained via the Department's bank. Departments should be aware however that the process of being approved and being allocated an OIN may take some time.

Additional information on the requirements and process for setting up a Payments Service can be found in the Gateway Payment Engine Business Implementation Guide.

4 Card Payment Processing

The following sections describe, in a logical (chronological) order, the processing that takes place from the capturing of the card details at the Department or LA website through to the posting of the authorised payment details to the Department or LA back-office system.

4.1 Capturing the Card Details

The capture of the card details for a payment is the responsibility of the Department or LA making the payment request for a Service. This enables the data capture screens to be designed and developed within the context of the business application to which the payment relates. It also enables the Department or LA to include business references that will link the payment being made to a record or customer in the back-office database. This is a business key and is not used by the Payment Engine.

The core business data required by the Payment Engine for a valid Payment Request comprises:

Service Name	*Mandatory*	The name of the Service which has been set up with the Gateway Payment Engine and for which the payment relates. This enables the Payment Engine to route the payment and associated notifications correctly
Payment Originator	*Optional*	An optional field for Departments and Local Authorities to identify the originator of the payment by name.
Card Number	*Mandatory*	The (typically 16 digit) card number sometimes referred to as the PAN
Start Date	*Optional*	Optional depending upon the rules in place from time to time for a specific card type or card issuer.
Expiry Date	*Mandatory*	The expiry date of the card
Issue Number	*Optional*	Optional depending upon the rules in place from time to time for a specific card type or card issuer.
Amount	*Mandatory*	The amount, to 2 decimal places, to be debited from the card.
Currency	*Mandatory*	The currency in which the payment is to be taken.
User Transaction Reference	*Optional*	A business reference used by the Department to link the payment to a customer or back-office record. There are 20 free-format User Transaction Reference fields available to the Department to use. The payment engine does not validate these fields.
The data below is captured for CV2AVS checking and can be left out if not required		
Policy	*Optional*	The policy is set according level of checking that is required by the payment service for CV2AVS
StreetAddress1	*Mandatory (if CV2AVS included)*	The first line of the street address
StreetAddress2	*Optional*	The second line of the street address
StreetAddress3	*Optional*	The third line of the street address
StreetAddress4	*Optional*	The fourth line of the street address
Postcode	*Mandatory (if CV2AVS included)*	The postcode for the street address
CV2	*Mandatory (if CV2AVS included)*	The card verification number (or security code) that is found on the back of the customer credit or debit card

Any other data collected by the Department or LA will be a requirement of the business processing associated with what is being paid for, but are not required items by the Gateway Payment Engine for the successful processing of a Payment Request.

Once the details have been captured by the website or portal they are translated into a payment request for submission to the Gateway Payment Engine in an agreed format (SOAP) and over a secure internet link (SSL).

4.2 CV2AVS checking

The Address and Security Code Verification Service (CV2AVS) allows the Card Holders Statement Address and/or the Card Security Code provided by the customer to be compared with the information held by the Issuer when the card payment is authorised. These can be checked to help identify and reduce the impact of fraudulent transactions.

For a CV2AVS transaction to be classed as successful, it must pass a minimum level of checking. This minimum level of checking is called the *policy*, and is set depending on the level of checking required by the payment service.

4.2.1 Policy Usage

The payment service chooses which policy to use as listed below.

Policy	Places Priority on	Accepts transaction if
2	CV2	The CV2 element has been checked and a successful match is made with the bank
3	AVS and CV2	All elements have been checked and a successful match for all elements is made with the bank
6	CV2	Either the CV2 element has been checked and matched or all elements returned not checked by the bank
7	AVS and CV2	Either all the elements have been checked and matched, or all elements returned not checked by the bank

4.3 Card Detail Validation

On receipt of a Payment Request from an authenticated source, the Gateway Payment Engine will carry out as much validation as possible on the request data. This validation includes ensuring that :

- The Service Name represents a valid Service set up within the Payment Engine
- The Card Number is in a valid structure
- The Start Date/Expiry Date/Card Number are present and correct according to the validation rules for the card type or card issuer **NB these rules are specific to card issuers and vary from time to time; Departments implementing card payments should check with eGU for the validation requirements current at the time of implementation.**
- The amount is syntactically correct and is within the Service limits set by the Department
- The currency is a valid currency for the Service.

And for CV2AVS checking are listed below:-

- If the CV2 number element is presented then it must be populated with numeric data (Applies to all policies)

-and-

- Dependant on the card type it must be the correct number of digits 3 or 4 (Applies to all policies)

- If AVS elements are presented then the StreetAddress1 must be presented and be populated (Applies to policies 3 and 7)

-and-

- The Postcode element must be presented and be populated with a valid UK postcode in a format outlined in the Govtalk e-gif standards found at http://www.govtalk.gov.uk/gdsc/schemaHTML/bs7666-v2-0-xsd-PostCodeType.htm (Applies to policies 3 and 7)

If any of the Payment Request data is invalid an error response is returned to the calling Department website. The Department is not charged for transactions that fail at this point unless the payment transaction is declined due to an in-correct CV2 number or AVS address.

If the Payment Request data has been successfully validated, a unique Payment Reference Number is allocated to the request, the request details are stored within the Payment Engine database and the request is passed to Datacash for authorisation.

4.4 Datacash Processing

On successful validation of the card details, the Payment Engine passes the Payment Request via a dedicated secure link to the Payment Service Provider – Datacash.

Datacash are responsible for obtaining, in real time, authorisation from the card issuer for the payment being requested. Prior to making the authorisation request to the card issuer, Datacash will carry out similar validation on the card details to that described in 4.2 above.

The card issuer will validate the card details and payment request and return either an authorisation code if the request was successful or a failure response if the request failed. Typically reasons for failure will include:

- Insufficient funds available on the card
- Card has been 'stopped'
- Card is stolen
- Card details do not match the card issuers records
- CV2AVS information does not match

Where the Payment Request has failed, Datacash will respond to the Payment Engine with a failure code. Where the Payment Request succeeds Datacash will respond to the Payment Engine with an Authorisation Code. In both cases, Datacash will also supply an additional reference number – BankRef – and a Time Stamp of when the request was approved. Both of these data items are important for the reconciliation process.

4.5 Payment Engine Response to Department Web Site

On receipt of authorisation for the Payment Request, the Payment Engine will log in the database the status of the Request and will store the additional data items supplied by Datacash – Authorisation Code, Bank Ref and Time Stamp.

The Payment Engine will then provide a response to the calling portal or web site with the a status code of 'successful', the Payment Reference, the Authorisation Code, the Bank Ref and the Time Stamp.

4.6 Payment Engine Response to Department Back-Office (non DIS)

Where a Department or Local Authority has no connection to the Government Gateway via a DIS box, it will be the responsibility of the Department portal or website making the Payment Request to capture the returned Payment information, (particularly Bank Ref and Time Stamp).

It will also be the Department's responsibility to implement (if required) the functionality to pass the payment details to the back-office systems for updating customer or financial records.

If the back-office system is not updated with payment details the Department will be relying on receipt of their bank statement to tell them a payment has been made. Customer records will not therefore be up to date.

4.7 Payment Engine Response to Department Back-Office (DIS only)

Where a Department or Local Authority is connected to the Government Gateway via a DIS box, an additional, real-time, notification will be sent by GGPE to the Departments DIS box of each authorised Payment Request (or Refund). This enables the Department to keep back-office customer records up to date. and will provide the Department with the ability to update financial systems automatically.

The Payment Notification will contain both the Bank Ref and the Time Stamp to support reconciliation.

4.8 Settlement of the Transaction

On receipt of an authorisation code from the card provider, Datacash add the Payment Request to a batch file of the day's transactions. The Time Stamp is used to determine which day's file a Payment Request will be added to, with all Requests received between midnight (00:00:00) and one second to midnight being included in the batch for that day.

Just after midnight the batch of authorised payments for the previous day is sent by Datacash to the bank to be settled.

The bank requests the funds from the card provider, and when received credits those funds to the Departments bank account. This process typically takes between one and three working days depending on bank processes.

The payment will then also appear on the customer's next credit card statement as normal. A Department may determine with their bank what reference should appear against the credit card statement entry, but this will be a Department or Service specific reference not payment specific.

4.9 Two-Step Payment Process

Departments and Local Authorities may, if they wish, adopt a two-step approach to payments comprising:

Step 1 – Pre-Authorisation

Step 2 – Fulfilment

This process is likely to be useful where a Department's business process dictates that there is a requirement to ensure that a payment can be taken (authorised) before embarking on a course of action, but that the actual payment may or may not be taken depending on the outcome of that action. An example might be an application for a permit, where a Local Authority needs to be sure that

payment can be made before validating the application, but will only request the money if the application turns out to be successful.

4.9.1 Pre-Authorisation

The process for pre-authorisation of a payment is exactly the same as for taking a payment and follows the flow as described in sections 4.1 to 4.6 above.

The difference however is that because a different API method is used to call the Payment Engine (and in turn Datacash), the Payment Request is not added to the daily batch for settlement. It is held in a suspense file until the second part of the process is received (the Fulfil request).

4.9.2 Fulfilment

The second part of the two-step process is for the Department or Local Authority to send a request to GGPE to fulfil a previously authorised payment, i.e. a request to transfer funds from a debit or credit card relating to a previously authorised transaction.

The original Payment Reference must be supplied in order to Fulfil a pre-authorised payment. On receipt of a valid Fulfil Request with a valid Original Payment Reference, Datacash will add the Payment Fulfil Request to that day's fulfilment batch.

A Time Stamp for the Fulfil transaction will be passed back to the calling application (via GGPE) to enable reconciliation of the daily batch totals to remain correct.

Notifications via the DIS box (where present) will be sent for both successful Pre-Authorisations and successful Fulfils to ensure back office customer and financial records can be kept up to date.

The length of time for which a Pre-Authorisation will remain valid varies from one card provider to another, but Switch is usually 24 hours and all other card issuers are usually up to 14 days Fulfilment requests sent after the Pre-Authorisation has expired will be rejected, and payment will not be made.

5 Direct Debits

The following sections describe, in chronological order, the processing that takes place from the capturing of the Direct Debit Instruction (DDI) Set-Up details at the Department or LA website through to the posting of Draw Downs against that DDI from the Department or LA back-office system.

GGPE supports a fully paperless Direct Debit Set-Up process, which means that there is no requirement for a signature from the Account holder (customer). There are however Direct Debit Scheme rules (owned and operated by BACS) that apply to the operating of a Direct Debit scheme by Departments, paperless or otherwise, and these should be reviewed with the Department's bank to ensure that the Department's business processes adhere to those rules.

5.1 Capturing the DDI Set-Up Details

The capture of the DDI Set-Up details is the responsibility of the Department or LA making the request to set up for a Service. This enables the data capture screens to be designed and developed within the context of the business application to which the payment relates. It also enables the Department or LA to include business references that will link the payment being made to a record or customer in the back-office database. This is a business key and is not used by the Payment Engine.

The core business data required by the Payment Engine for a valid DDI Set-up Request comprises:

Service Name	*Mandatory*	The name of the Service which has been set up with the Gateway Payment Engine and for which the DDI relates. This enables the Payment Engine to route the DDI and associated Draw Downs correctly
Account Number	*Mandatory*	The (typically 10 digit) number identifying the customer's bank account.
Sort Code	*Mandatory*	The (typically 6 digit) number identifying the sort code associated with customer's bank account. The sort code identifies the bank and branch.
Account Name	*Mandatory*	The name of the Account holder.
Imported Instruction ID	*Mandatory (for imported instruction only)*	Where a DDI has been imported into the Payment Engine having been set up elsewhere, the instruction ID number must be supplied.
User Transaction Reference	*Optional*	A business reference used by the Department to link the DDI to a customer or back-office record. There are 20 free-format User Transaction Reference fields available to the Department to use. The payment engine does not validate these fields.

Any other data collected by the Department or LA will be a requirement of the business processing associated with Service for which the DDI is being set up, but are not required items for the successful processing of a DDI Set-Up Request.

Once the details have been captured by the website or portal they are translated into a payment request for submission to the Gateway Payment Engine in an agreed format (SOAP) and over a secure internet link (SSL).

5.2 DDI Set-Up Validation

On receipt of a DDI Set-Up Request from an authenticated source, the Gateway Payment Engine will carry out as much validation as possible on the request data. This validation includes ensuring that :

- The Service Name represents a valid Service set up within the Payment Engine

- There is a valid Originator's Instruction Number (OIN) associated with the Service
- The Account Number is in a valid structure
- The Sort Code is in a valid structure
- The Imported Instruction ID (if present) is in a valid structure.

If any of the DDI Set-Up Request data is invalid an error response is returned to the calling Department website.

If the DDI Set-Up Request data has been successfully validated, a unique reference number is allocated to the request, the request details are stored within the Payment Engine database and the request is passed to Datacash for processing.

5.3 Datacash DDI Set-Up Processing

On successful validation of the request details, the Payment Engine passes the DDI Set-Up Request via a dedicated secure link to the Payment Service Provider – Datacash.

Datacash is responsible for obtaining authorisation from the customer's bank (via BACS) for the DDI to be set up. Prior to making the authorisation request to the bank, Datacash will carry out similar validation on the request details to that described in 5.2 above.

The BACS and bank validation of the request are not real-time. This process will take several days, and Departments cannot request Draw Downs against a DDI for a minimum of 5 working days from Set-Up request.

The bank will validate the account details and set-up request and if successful BACS will return a DD Instruction ID to Datacash.

Typically reasons for failure will include:

- Incorrect Account Number and Sort Code combination
- Account does not exist (or has been closed)
- Account has been suspended
- Account type does not support Direct Debits
- Incorrect Name associated with Account

Where the DDI Set-Up Request has failed, Datacash will respond to the Payment Engine with a failure code.

5.4 Payment Engine Response to Department Web Site

The Payment Engine will provide a synchronous response to the calling portal or website but this response will only indicate that that the request has been received successfully and has passed initial validation (or otherwise).

Because the BACS and bank processing of the DDI Set-Up request is not real-time, the Payment Engine cannot provide a synchronous response to the calling portal or web site to indicate whether the set up was successful or not. It will be the Department's responsibility to inform the end User of failures.

5.5 Payment Engine Response to Department Back-Office (non DIS)

Where a Department or Local Authority has no connection to the Government Gateway via a DIS box, it will be the responsibility of the Department portal or website making the DDI Set-Up Request to capture any request information.

It will also be the Department responsibility to implement (if required) the functionality to pass the DDI Set-Up details to the back-office systems for updating customer or financial records.

If the back-office system is not updated with DDI details the Department will not be aware that a DDI has been set up for a customer and will not therefore be able to make any Draw Downs against it.

5.6 Payment Engine Response to Department Back-Office (DIS only)

Where a Department or Local Authority is connected to the Government Gateway via a DIS box, an additional, real-time, notification will be sent by GGPE to the Department's DIS box of each authorised DDI Set-Up Request. This enables the Department to keep back-office customer records up to date. and will provide the Department with the ability to update financial systems automatically.

The Payment Notification will contain the DDI Reference Number to support the Draw Down process.

5.7 Draw Downs

Once a DDI has been successfully set up, Departments and Local Authorities can make Draw Downs against that DDI i.e. they can request that funds are transferred from the customer's bank account to the Department's bank account under the authority of the DDI and subject to DD Scheme rules.

The Draw Down method is currently only available via a DIS box connected to Government Gateway on the basis that the business logic to support the triggering of Draw Downs will be held in the back office financial or customer management system and not the portal. It will therefore be these back office systems that trigger Draw Down requests.

A Draw Down requires the following data to be provided to GGPE by the Department:

Service Name	*Mandatory*	The name of the Service which has been set up with the Gateway Payment Engine and for which the DD relates. This enables the Payment Engine to route the Draw Down correctly
DDI Reference	*Mandatory*	The reference number of the DD Instruction against which this Draw Down is being made.
Amount	*Mandatory*	The amount (to 2 decimal places) to be debited from the customer's account.
Due Date	*Mandatory*	The date on which the amount is to be debited.
User Transaction Reference	*Optional*	A business reference used by the Department to link the DD to a customer or back-office record. There are 20 free-format User Transaction Reference fields available to the Department to use. The payment engine does not validate these fields.

On receipt, the Payment Engine will validate the Draw Down request to ensure that:

- The Service Name represents a valid Service set up within the Payment Engine
- The DDI Reference number corresponds to a valid DDI on the Payment Engine database
- The Amount is syntactically valid
- The Due Date is syntactically valid and is at least 3 working days in the future

If the Draw down passes this initial validation it is logged and passed to Datacash for processing.

Datacash will perform similar validation, and if successful will add the Draw Down request to the daily batch file for submission to BACS. BACS processing is not real-time, therefore there is no synchronous response from BACS to Datacash, Datacash to GGPE, or GGPE to Departments.

BACS will process the Draw Down on the Due Date in accordance with the DD scheme rules. Any subsequent failure to process the Draw Down (account closed since DDI set up for example) can be reported to the Department by the bank. A separate report (ARRUD) is available to Departments by negotiation with their bank, although there is normally a charge associated with this report. Reporting of Draw Down failures is outside the scope of the Payment Engine.

6 Refunds

Refunds can be made against any payment or DD Draw Down made through the Payment Engine. Refunds can be made using the Helpdesk Application (see 8 below) which ensures that some control over the refund process can be maintained by the Payment Engine, and Departments can control who in their organisation has access to the refund functionality.

In addition a Secure Refund function is available that allows card payment refunds to be made outside of the Helpdesk application (see 7 below)

The Payment Engine applies the following limitations to the Refund process:

- A Refund can only be made against a payment previously made through GGPE. This Payment must be identified by Payment Reference (although can be searched for via the Help Desk Application using wider criteria such as last 5 digits of card number – see Section 7 below).
- The refund amount cannot exceed the original payment amount.
- Multiple Refunds can be made against a single payment, but the total of the multiple refunds cannot exceed the amount of the original payment.
- Refunds may be made against both card payments and DD Draw Downs
- A refund cannot be made against a Pre-Authorised payment that has not yet been Fulfilled.

The process for Refunds follows the same logic and pattern as that for a standard card payment, and is processed by Datacash in the same way with regard to daily settlement batches and time stamping.

Refunds also generate a Notification message which is sent to the Department back office systems via a DIS box (where present) to ensure customer and financial systems are kept up to date. Note that where a non-DIS implementation is used, a Refund Notification cannot be sent.

7 Secure Refunds

A Secure Refund capability is available via SOAP API. This is achieved by supplying a unique username and password to the Customer organisation wishing to use the function for their payments service coupled with a secure connection using certificates. Secure Refunds have the same processing and rules restrictions as Refunds made via the Helpdesk Application.

Validation checks are performed before allowing the Refund to be processed. Failure will occur if :

- the credentials (user name and password) supplied to use the service are not valid
- the payment service has not been set up to use the secure refund function
- the refund does not match a payment that has already been processed

This will stop refunds being processed that do not have the correct authority.

8 Payments Helpdesk Application Functionality

A Payment Engine Helpdesk Application is available to Departments and Local Authorities to support their use and management of their Payments Service. It will be essential for any Department or Local Authority providing any form of telephony or call centre support to the public or their customers with regard to the Service to which the payments relate.

The Helpdesk Application is available to any authorised user via either internet or GSI. It will be for the Department to determine user authorisation, and access will be via a user id and password regime over a secure (SSL) connection.

Functionality available within the GGPE Helpdesk Application includes:

- Make a new Card Payment
- Query Card Payment by Last 5 digits of Card Number
- Query Card Payment by Payment Reference
- Query Card Payment by (primary) User Transaction Reference
- Request Set-Up of New Direct Debit Instruction
- Import Existing DDI
- Query DDI by Account Number
- Query DDI by DDI Reference
- Query DDI by User Transaction Reference

Details of failed Payment Requests are not available for view from the Help Desk.

Additionally a transaction level report is available from the Help Desk for card payments and can be requested for any given time period (by specifying start and end periods for the report). The report is delivered to the desktop from which it was requested and is delivered as a CSV file so that it can be easily imported into a spreadsheet or automated process to support reconciliation. The report contains the following payment data for each successful payment request within the time frames requested:

- Payment Type
- Payment ID
- Original Payment ID
- Amount
- Currency
- Last 5 Digits of Card No
- Card Type
- Auth Code
- User Txn Ref
- Originator
- Time Stamp

More details on the Payment Engine Help Desk Application and how to use it can be found in the document Government Gateway Helpdesk Application - Payment Function User Guide for Helpdesk Advisors available from EDT.

9 Miscellaneous Functionality

9.1 Reconciliation of Bank Totals

The Payment Engine does not have any specific functionality to do the reconciliation of daily totals with bank totals on behalf of a Department or Local Authority. This is because the Payment Engine supports multiple Merchant Acquirers (banks) and provides a feed to multiple platforms for Back Office system integration. As a piece of Common Infrastructure, providing flexibility to Departments and Local Authorities, it is not possible for the Payment Engine to support every combination of banks and systems.

It does however provide key components to support the Reconciliation process, including:

- Transaction Level MIS Report from Help Desk.
- Consistent Time Stamping throughout to clearly define daily settlement batches
- Return of Bank Ref for consistency of referencing throughout process (Bank Ref is the reference which the bank will hold for each transaction)
- SOAP Response to Portal following Payment Request (includes both Bank Ref and TimeStamp as well as Payment Ref and Auth Code)
- Notifications (XML) via DIS box (where implemented) of payment request. Includes Bank Ref and TimeStamp as well as Payment Ref and Auth Code. Will also include any User Transaction References for easy matching to Back Office (e.g. CRM) records.

Departments and Local Authorities are advised to consider how, from an organisational perspective, the reconciliation process will be carried out, and in particular to ensure that routes for exploring any reconciliation failures are clearly understood. The Payment Engine provides a route to transaction level detail within both the core Payment Engine and Datacash.

9.2 Time Outs

To ensure that the integrity of the payment processing cycle is maintained should a response to requests across system components not receive a response, the Gateway Payment Engine has a cascading time out sequence across all the components of the architecture to ensure that the situation is handled effectively.

These time outs are:

Request Made By	**Request Made To**	**Time Out Period**, following which calling application should assume error if no response received.
DataCash	Authorisation Body (Card Provider)	30 seconds (actual)
Gateway Payment Engine	Datacash	45 seconds (actual)
Dept/LA Portal or calling application	Gateway Payment Engine	60 seconds (recommended)

9.3 Duplicate Payment Checking

In order to identify and trap potential Denial of Service attacks, the Payment Engine will identify and prevent duplicate payments being made within a specific time frame. The criteria for identifying payments as duplicates is intended to avoid any impact on genuine payment requests but at the same time trap any unusual behaviour.

For the purpose of this check, duplicate payments are deemed to be:

- A payment received within **two** seconds of a previous payment with the same card number.
- A payment received within **ten** seconds of a previous payment with the same card number and same amount.

This duplicate check is not however intended to capture duplicate submissions of the same payment made in error at the portal or by the User. These should be handled by portal processing (e.g. disabling of the “submit” button or equivalent until response received from initial request).

Appendix A - Additional Information

Additional information on the Government Gateway Payment Engine can be obtained from the e-Delivery Team within the Cabinet Office e-Government Unit (eGU) or from any of our partner organisations supporting payments solutions using the Gateway Payment Engine:

Sun & SoftwareAG	(www.softwareag.co.uk)
Etude Consulting	(www.etude.com)
Microsoft	(www.microsoft.com)

As well as product specific specialist knowledge to support the definition of your business requirements and understanding of how the Payment Engine can you support you, eGU will also appoint a Service Implementation Manager to help Departments and Local Authorities through the testing and implementation phases of the project.

The e-Delivery Team within eGU team can be contacted via email at:

edt@cabinet-office.x.gsi.gov.uk

Additionally the following documentation is available from e-Government Unit to help understand what will be required to implement the Gateway Payment Engine:

QP04 Gateway Payment Engine Questionnaire

Gateway Payment Engine Business Implementation Guide

Gateway Payment Engine - SOAP Programmatic Interface Specification

Gateway Payment Engine – Notification Interface Specification

Gateway Payment Engine – Programmatic Interface Specification

Gateway Gateway Helpdesk Application – Payment Function User Guide for Helpdesk Advisors