The Government Gateway

Release 1.5
Contents

THE GOVERNMENT GATEWAY ..................................................................................... 5
  PURPOSE .................................................................................................................. 5
  BACKGROUND ........................................................................................................ 5
  THE GATEWAY ........................................................................................................ 6
  BENEFITS ................................................................................................................ 6

CONCEPTUAL OVERVIEW ....................................................................................... 8
  GATEWAY CORE MODULES .................................................................................. 8
  GATEWAY ADDITIONAL MODULES ...................................................................... 8
  CONNECTIVITY ........................................................................................................ 9
    GSI Connections .................................................................................................. 9
    Internet-based Connections ............................................................................... 9
    SSL-based connection ........................................................................................ 9
    VPN-based connection ....................................................................................... 9
  REGISTRATION AND ENROLMENT ....................................................................... 9
  TRANSACTION ENGINE ........................................................................................ 10
  DEPARTMENTAL INTEGRATION SERVICE .............................................................. 10
  SECURE MESSAGING ............................................................................................ 11
  HELPDESK ............................................................................................................. 11
  PAYMENTS ............................................................................................................. 12

GATEWAY USAGE SCENARIOS .............................................................................. 13
  INDIVIDUAL GOVERNMENT DEPARTMENT ......................................................... 13
    Single Sign-On ................................................................................................... 13
    Transactions ...................................................................................................... 14
    Inter-Organisation Messaging ........................................................................... 14
    Joined-up Transactions ...................................................................................... 15
  LOCAL AUTHORITY ................................................................................................ 15
    Single Sign-On ................................................................................................... 16
    Driving Uptake .................................................................................................. 16
    Transactions ...................................................................................................... 17
    Inter-Organisation Messaging ........................................................................... 18
    Joined-up Transactions ...................................................................................... 19

A 10 STEP GUIDE TO GETTING ONLINE USING THE GOVERNMENT GATEWAY ....20

  BACKGROUND ....................................................................................................... 20
  THE 10 STEPS TO E-SERVICE DELIVERY ............................................................ 20
    Step 1 - identify the services to be offered ......................................................... 20
    Step 2 - identify rules and key information resources for the service ................. 21
    Step 3 - decide which Gateway components to use ........................................... 21
    Step 4 - develop, or re-use, a suitable form (XML schema) ................................ 22
    Step 5 - install and configure Gateway connection and integrate to existing systems 22
    Step 6 - build and test the application ................................................................ 22
    Step 7 - prepare the Helpdesk and live services teams ...................................... 22
    Step 8 - certify the application ......................................................................... 23
    Step 9 - provide release data to the Gateway ..................................................... 23
    Step 10 - launch the service .............................................................................. 23
  SUMMARY .............................................................................................................. 23

GATEWAY FEATURES .............................................................................................. 24

  REGISTRATION AND ENROLMENT ........................................................................ 24
    Known Facts ....................................................................................................... 24
    Supported Types of User .................................................................................... 25
      Individual (Citizen) ......................................................................................... 25
      Organisation (Business) .................................................................................. 25
      Agents (Intermediaries) ................................................................................... 26
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDITIONAL GATEWAY FEATURES</td>
<td>44</td>
</tr>
<tr>
<td>SECURE MESSAGING</td>
<td>44</td>
</tr>
<tr>
<td>User-Initiated Communication</td>
<td>44</td>
</tr>
<tr>
<td>Government Organisation-Initiated Communication</td>
<td>44</td>
</tr>
<tr>
<td>View Inbox</td>
<td>44</td>
</tr>
<tr>
<td>Create New Mail</td>
<td>45</td>
</tr>
<tr>
<td>Sent Messages</td>
<td>47</td>
</tr>
<tr>
<td>Notifications of new secure messages</td>
<td>47</td>
</tr>
<tr>
<td>HELPDESK</td>
<td>48</td>
</tr>
<tr>
<td>PAYMENTS</td>
<td>48</td>
</tr>
<tr>
<td>APPENDIX A – STANDARDS</td>
<td>49</td>
</tr>
<tr>
<td>APPENDIX B – DEVELOPER INFORMATION</td>
<td>50</td>
</tr>
<tr>
<td>APPENDIX C – POTENTIAL FUTURE ENHANCEMENTS</td>
<td>51</td>
</tr>
</tbody>
</table>
The Government Gateway

Purpose

This document provides an overview of the features and services made available by the UK Government Gateway. It explains how these various services and interfaces can be used by government organisations, citizens and businesses.

The overall purpose of this document is to provide an overview of:

- **what** the current release of the Gateway does, by describing its components and facilities
- **how** to take advantage of its services, with a range of illustrative business scenarios that draw upon the Gateway’s components

Background

The government has established an ambitious strategy for electronic service delivery with several key objectives:

- 50% of transactions to be available electronically by 2002 and 100% by 2005
- customer centric public services
- joined-up services
- secure and trusted services

The aim of electronic service delivery is to provide better, customer driven and more efficient public services. Enabling citizens and businesses to transact electronically with government agencies is a key part of delivering this strategy. The Internet is being used as the core delivery channel for enabling these improvements in online service delivery. With its widely accepted open interoperability standards, the Internet provides an effective means of providing electronic relationships – both between government organisations, and between government organisations and their customers.

The major enabler of this UK-wide strategy is the Government Gateway. The Gateway provides:

- **authentication and authorisation services** – to ensure that users are who they claim to be and that they have the right to access a specific service or set of services
- **a single sign-on facility and single user credentials supported across all government services, national, regional and local** – meaning that users can have one user ID and password, or a digital certificate, which they can use for all online public services
- **a common transaction and routing facility** – ensuring the reliable delivery of documents and messages. This includes both documents between business and citizens and government, as well as the routing of documents between government organisations
- **a secure messaging facility** – enabling secure communication between business, citizens and government organisations
- **an integration tier** – offering reliable delivery of standards-based information into the connecting organisation, including the option for customised local integration into existing systems and applications
- **a payments facility** – offering payments ranging from credit and debit cards through to direct debit

The Gateway is part of the UK’s critical information infrastructure and provides a highly secure environment, a resilient “always on” service and a capacity to handle high volumes.
The purpose of developing this common infrastructure shared across national, regional and local public services is to:

- avoid the duplication of the common facilities and services necessary to connect individual organisations to each other and to customers over the internet
- deliver joined-up services by providing a common authentication service
- enable a customer to interact with many government organisations in a single transaction using a single identity
- enable both the private and public sector to provide customer-driven applications that can interact with government in a consistent manner

**The Gateway**

The Gateway acts as an intelligent hub. It is responsible for providing authentication services, verifying the integrity and validity of submitted transactions and for routing them to or between appropriate government organisation(s).

Over time, it is anticipated that the Gateway will handle the majority of the estimated 5-6 billion of annual government-related transactions. The Gateway has a goal of providing a minimum of 99.95% availability, which may move to 99.999% availability as it becomes an increasing cornerstone of government business.

The Gateway facilitates joined-up working between all stakeholders. This allows government organisations to communicate with their electronic business users and citizens using the same, consistent mechanism. The Gateway infrastructure also enables them to communicate between themselves – so a central government department, for example, can use the Gateway to securely route forms to a local authority. Hence the potential user community is in excess of 30 million citizens, agents and businesses. The number of national, regional and local government organisations is estimated to be in excess of 1,000.

**Benefits**

The benefits of using the Government Gateway include:

- **a reduction in the costs to e-enable services** – core Gateway functionality such as single sign-on, secure two way electronic communication, common document authentication and routing, open standards and multi-platform support, and support for multi-channel delivery through open interfaces ensure that public sector organisations do not need to develop their own solutions for transactions, secure e-mail, authentication etc. Instead they can call into and make rapid use of these common Gateway services.

Indicative costs for designing a web site that provides these types of facilities are between £1M and £3M or more, and this does not include the costs associated with hosting and supporting the site. Implementing a digital signature signing capability can cost up to £250,000 per instance along with additional costs of £40,000 for each new certificate provider (presently there are two certificate providers already supported by the Gateway, with two more already coming on board and with more expected, taking the anticipated total to over ten). Each organisation would face those costs alone if the core infrastructure is not used. More importantly, there can be no cross-government authentication unless there is a single virtual record that all public sector organisations can trust. The Gateway hence reduces the costs of implementation, reduces risk and decreases project delivery time-scales

- **a proven way of inter-connecting back-office systems securely** – the Gateway provides a cost effective and fast way for connecting existing systems using open interoperability standards compliant with the e-Government Interoperability
Framework (e-GIF)

- **single sign-on and masking of back-office structures** – the Gateway delivers joined-up transactions where one customer service can be directed to many parts of government. The complexity of back-office systems are masked from the citizen and business.

- **a reduction in the time to deliver projects** – organisations can narrow the scope of the work required to deliver e-services since the Gateway already delivers part of the solution. Their focus can be on e-delivery of core services, rather than on all the peripheral components (such as authentication, payments etc) that sit around the service.

- **the ability to deliver customer centric projects** – the Gateway provides the infrastructure to enable joined-up transactions. This enables citizen- and business-focused services to be developed, regardless of the number of departments or Local Authorities that are involved in the process.

- **interoperability** – through GovTalk, the UK Government’s data interoperability standard which uses W3C standards and complies with the e-GIF, the Gateway promotes best practice on the use of XML and schema creation to provide interoperability based on open standards.

- **others** – savings in running costs as more services are delivered; reduction in fraud; savings from reduced print, production and postage costs; the cost of delivery by leveraging central infrastructure is likely to be 25-35% of silo-based implementation; joined up processes reduce overhead throughout government.
Conceptual Overview

The Gateway was designed to simplify and accelerate the UK e-Government programme. It achieves this by ensuring that the common building-block components of e-Government services are provided once, in a flexible, modular and scalable way.

The Gateway provides a common foundation for authenticated interactions and transactions between citizens, businesses and Government organisations:

It is the responsibility of government organisations, as part of their e-Government strategies, to develop e-GIF (e-Government Interoperability Framework) compliant transactions that can be accepted electronically by the Gateway and, in conjunction with the Gateway service provider, to devise the business rules associated with each type of transaction.

As the Gateway uses entirely open interoperability standards – XML, HTTP, SOAP and W3C digital signatures combined with X509 certificates – and is fully aligned with the e-GIF, the process of developing and enabling electronic transactions is simplified.

Gateway Core Modules

The Gateway has been designed around three main core modules:

- **Registration and Enrolment (R&E)** – providing the authentication and authorisation services, enabling single sign-on across all government-related sites
- **Transaction Engine (TE)** – providing a common transaction authentication and routing infrastructure
- **Departmental Integration Service (DIS)** – providing reliable open-standards (SOAP/XML) two-way communication between organisations and the Gateway together with potential application integration features (mapping between XML and local data formats)

Gateway Additional Modules

In addition to its core functions, the Gateway also provides a range of associated services. These are:
- Secure Messaging – providing a secure two-way communication channel (webmail) between government organisations, businesses and citizens
- Helpdesk – providing a service for government organisations making use of Gateway-powered services
- Payments – providing a central payments service, either used standalone or embedded as part of a larger transaction. It supports credit cards, debit cards and direct debits. It is anticipated that payments will go live in the 1.6 release timeframe.

**Connectivity**

For casual use, by the general public and most businesses for example, connection to the Gateway is via the Internet. For those who exchange information on a more frequent basis and who offer services via the Gateway, a dedicated means of connection and communication is required. The Gateway supports two options.

**GSI Connections**

Those departments and other government organisations that have a Government Secure Intranet (GSI) connection can use that to establish their links with the Gateway. This is shown in the diagram below.

![GSI Connection Diagram]

**Internet-based Connections**

The alternative method of connection for those not on the GSI is via the Internet, using either SSL or dedicated VPN equipment. Generally it is anticipated that the SSL option above will be used.

**SSL-based connection**
Secure Socket Layer (SSL) based, mutual authentication connections enable a connecting organisation to use industry-standard protocols to make its dedicated connection to the Gateway. This is shown in the diagram below.

![SSL Connection Diagram]

**VPN-based connection**
Virtual Private Network (VPN) connections provide a means of establishing a dedicated connection to the Gateway using specific equipment. There is only one recommended supplier of VPN equipment at the present time, Barron McCann. The use of VPN is shown in the diagram below.

![VPN Connection Diagram]

**Registration and Enrolment**

The Registration & Enrolment (R&E) system is the part of the Gateway that enables users to set up their single sign-on credential. This can be either a password and User ID, or make use of digital certificates. R&E provides:

- a web-based user interface (a set of pages for use by online users)
a web service, programmatic interface (to make use of Gateway services directly from within portals, web sites and other applications, such as desktop application software)

It manages:

- the process of registration of client credentials (User ID/password or digital certificate) with the Government Gateway
- the matching and verification of unique user identification information against the authentication data provided by government organisations
- enrolment into services
- the ongoing management of the registration and enrolment data

and communicates with the organisation’s own systems via XML messages sent over either the Government Secure Intranet (GSI) or the Internet.

The process of enrolment involves proving entitlement to any given service. It provides:

- a method whereby a government organisation can control which of their services are available to which of their customers
- an opt-in and opt-out mechanism for users to choose which services they want to carry out electronically with government
- a security mechanism to prove entitlement to any given service
- a mechanism to prove authority to act on an organisation’s behalf by a recognised member of an organisation

The R&E system accepts requests from the Transaction Engine for authentication of credentials (is the presented credential valid and registered with R&E?) and authorisation checks (is the credential allowed to access a particular service?)

Credentials can be very secure: digital certificates, which can ensure non-repudiation when used for signing; or User ID/Password combinations according to the security need defined by the organisation.

Transaction Engine

The Transaction Engine (TE) authenticates and routes transactions (which are typically XML business forms and documents) destined for various government organisations. These transactions may be prepared by clients interacting with web sites and portals through a browser, or by applications installed on client computers. Either way, the completed transaction is either used with a User ID/Password or digitally signed on the client computer and sent to the Government Gateway over the Internet as an XML formatted document. Internet-standard HTTP (under 128 bit SSL) is used to submit the document to the Gateway.

The Transaction Engine verifies the integrity of the received signed request, calls the R&E service to authenticate the credential used and confirm that the requested transaction is authorised for this credential, and then routes the transaction to the appropriate organisation for processing.

Departmental Integration Service

The Departmental Integration Service (DIS) provides connectivity and facilitates two-way communication between the Government Gateway and departmental systems. It uses open standards, namely XML, HTTP and SOAP.

In order to be able to carry out electronic business transactions and communicate with their customers over the Internet, government organisations must be able to link their existing IT environment successfully with the Government Gateway. DIS facilitates this function by providing an interface between an organisation’s local servers and the Gateway,
The Government Gateway – Release 1.5
(Version 29.05.02)

guaranteeing two-way communication and once-only delivery of documents between the two. It also provides an audit trail of Gateway transactions, showing their safe receipt/dispach.

A high-level overview of how DIS installations interact with the Gateway is shown below. In this case, the GSI is shown as the communication network between the Gateway and the connecting organisation, but the Internet can also be used as described earlier.

Secure Messaging

Secure Messaging enables secure two-way electronic dialogue between citizens and government and between businesses and government. A secure “webmail” mailbox is automatically created for all new users and assistants created on the Gateway, irrespective of authentication level.

The mail system is browser based. 128bit SSL is used to ensure protection of the communication channel between the user and the secure messaging system. Access to the system relies upon the Gateway’s authentication and authorisation service, ensuring the same single sign-on credentials can be used.

Rather than sensitive or confidential documents being sent out over the Internet, where it is difficult to guarantee their security and almost impossible to ensure guaranteed delivery, users are instead able to interact directly through a browser. Users can view their messages and respond to them securely all within the secure messaging facility.

Since secure messaging is exposed as a web service, it can also be hosted within an organisation’s own portal. A user can then interact with the messaging system within that portal rather than needing to visit the Gateway.

Additional service specific Terms and Conditions of the mailbox do not reside on the Government Gateway but are held on the appropriate organisation’s website. For example there are Terms and Conditions for PAYE on the Inland Revenue website and Terms and Conditions for VAT Returns on the HMCE website. The service-specific Terms and Conditions also describe the outgoing forms and statements that users should expect to receive electronically in their mailbox.

Helpdesk

Helpdesk support is provided by a web application. Access is controlled by User ID and Password. Each connecting organisation has a Helpdesk administration user. This administration user sets up Helpdesk users within their own organisation as users of the system. During this set up, the details of the user will be recorded and they will be given access to the Helpdesk functions that they require. Day to day users are likely to have fewer functions available than more experienced investigative types of users.

- Page 11 -
The main features provided by this system include:

- **Helpdesk administration**: the setting up and maintenance of users within departments and other government organisations that are allowed to use the functions of the helpdesk support system
- **User Maintenance**: allows the amendment of Gateway user details such as the allocation of an agent for a user or requesting the issue of a new password for a user who has forgotten their old one
- **User enrolment support**: this allows enquiries on the status of the relationship of a user such as details of when the user enrolled and when they activated the service
- **User queries**: allows the query of information such as events that have occurred for a particular user or individual submission (transaction) details

**Payments**

The payment facility provides a flexible general payments service for all government organisations. This allows a call to be made from a portal/application to make a payment to a department by debit card, credit card or direct debit.

Payment functionality is triggered by a SOAP call made from the portal/application to the payment facility that processes a real-time authorisation and returns the result. This is a synchronous process.

Note: This facility is open to all – a user does not have to register in advance to make a payment.

This service is anticipated to go live with version 1.6 of Gateway.


**Gateway Usage Scenarios**

In order to understand the purpose of the various Gateway components and services detailed in this document, it is useful to put them in a business context and show them being exploited in a range of potential scenarios.

**Government Department**

As is made clear elsewhere in this paper, the Government Gateway provides a range of components, some or all of which may be relevant to a particular department. A high level overview of how a government department might make use of these common e-government components is shown below:

In the above, the department portal is:

- making use of the single sign-on facilities for its users
- using the ability to submit transactions to and from multiple parties
- taking outputs and contents from the secure messaging area and rendering them in their own portal

It is also using the payments engine, which supports online payments (debit cards, credit cards or direct debit facilities).

**Single Sign-On**

A department may choose initially to take advantage of the single sign-on facilities offered by the Government Gateway. This enables users to set up a User ID and password (or digital certificate if that is required for services) for use with the department’s portal and services. The same identity will also be usable with all the other services powered by Government Gateway single sign-on. Using this single identity, the department can personalise their services around a user, enabling them to establish a strong customer-relationship, while also enabling support for a common secure credential that can be used across all government services.

The common single sign-on facility of the Gateway is a key component of delivering joined-up government since users (both citizens and businesses) are able to use the same User ID/Password or digital certificate across the entire spectrum of government services.
Transactions
Another use of the Gateway by a government department is for all of its transactions, as shown below.

This enables the department to offer a rich portfolio of services, with its attention focused on the delivery of business value to its key customers rather than in the unnecessary construction and duplication of common infrastructure components.

Walking through this, a user can submit a business form to the Gateway. It will then be authenticated and routed to the appropriate department. The department then processes the form and returns any resulting statement or other response document to the originator's secure messaging store. The user can either read that response online (and initiate further correspondence relating to it should they so wish) or it can be accessed by application software and processed within that application.

Inter-Organisation Messaging
The Gateway also provides an infrastructure for authentication and messaging between organisations, such as between one government department and another, or between a government department and a local authority. This enables the common infrastructure to be used to move documents and communications between different government organisations –
for example, a local authority could communicate with a central government department or a private pension company make automatic electronic returns to say the DWP.

This is shown in simplified form below.

As with externally-originated transactions, transactions between government organisations and related parties are also authenticated and automatically routed by the Gateway. The authentication and authorisation features of the Gateway ensure that all communication flows are fully authenticated and authorised during these inter-organisation information exchanges.

The Gateway provides a common infrastructure to enable government departments to communicate in a secure, authenticated fashion with other parties, such as other local authorities, government departments and other Gateway-connected parties. Given the range of stakeholders and various parties that a local authority needs to communicate with, the Gateway provides a cost-effective and streamlined means of facilitating these connections and interactions.

**Joined-up Transactions**

The Gateway also supports joined-up transactions. Rather than each connecting organisation merely replicating its existing paper-based forms, users can be offered a single form that integrates various existing paper processes into a more streamlined approach. A single consolidated form completed online by a user can then be de-composed into its component parts and each handled in accordance with existing processes by a government department or departments. This is shown in overview in the diagram below.

**Local Authority**

As is made clear elsewhere in this paper, the Government Gateway provides a range of components, some or all of which may be relevant to a particular local authority. These are considered below.
Single Sign-On
A local authority may choose initially to take advantage of the single sign-on facilities offered by the Government Gateway. This will enable users to set up a User ID and password (or digital certificate if that is required for services) for use with their local authority portal and services. The same identity will also be available for use with all the other services powered by Government Gateway single sign-on.

Using this single identity, the local authority can personalise their services around a user, enabling them to establish a strong customer-relationship, while also enabling support for a common secure credential that can be used across all government services. An initial scenario could be a local authority portal using the Gateway for single sign-on services, and serving all of its own data, e-forms and interactions locally. This is shown in the schematic below.

Driving Uptake
One of the key issues with making e-government initiatives successful is driving uptake – that is, making services easy and compelling enough for citizens and businesses to want to interact electronically. The design of the Government Gateway recognises these concerns and provides a variety of features that can assist with the promotion and uptake of e-services.

In the single sign-on scenario the question arises of how and when a user would register and enrol for services in the first place – and hence how they would set-up their single identifier for use across all government services: local, regional and national. One method the Gateway supports is a promotional campaign by a government organisation. For example, a local authority could decide to promote e-services to all or some of its population through a concerted marketing and promotional campaign.

Let’s take the example of a local authority that is launching a range of local services – such as Council Tax statements and payments online, housing rent statements, payments and repair requests online, a clearing system for local school waiting lists online – and wishes to maximise uptake. It can do this through a range of awareness-raising materials on local authority premises – libraries, the town hall and so on – together with a mailshot to all targeted households.

Using its own databases, which contain information about each individual at a particular address and their relationship with a local authority (eg. Council Tax payer), the local authority can send out to its targeted audience letters which contain details of the new service(s) being launched, together with what is known as a Departmental Activation Token (DAT).

The letter would provide details of the service, the web address at which it can be found and alternative ways in which a user can make use of on-line services if they do not themselves have direct Internet access (such as for example making use of free Internet access PCs located in libraries).

To illustrate this, a letter might contain something along the example below. This is purely for illustration only and is not meant to be definitive in terms of the type of data that an authority might use in setting up suitable authorisation.
Dear Mrs ABC,

We are pleased to announce a new range of our services are now being made available on the Internet.

From today you will be able to access and make use of the following services, securely, over the Internet:

- **Council Tax**: statements and payments online
- **Education**: local schools co-ordinated waiting list clearing system
- **Street Amenities**: reporting of defective street lights, potholes in roads and other issues you wish to bring to our attention
- **Planning**: filing of planning applications online and online monitoring of progress

Contained in the sealed section of this letter is a secure PIN that will enable you to activate your online account and start using these new services. You will need to remove the secure flap at the base of this letter to access this PIN. Once your account is activated, you will then be set up ready to use these new services over the Internet.

If you do not have the facilities to directly access the Internet yourself, then all local branch libraries and the Town Hall have free use access terminals which you can use to make use of these services. Alternatively we are working with other organisations, such as the CAB, to enable them to access these services on your behalf should you wish them to do so.

To address any concerns about confidentiality you may have, please rest assured that these services use state of the art security features. The council is committed to ensuring the continuing privacy, confidentiality and integrity of all personal data in its possession.

If you have any questions about these new services, please contact our Internet Service Helpdesk on xxx xxxx xxxx or email eservices@localauthorityname.gov.uk.

As well as the activation PIN contained in this letter, in order to activate your online account you will also need the following information:

- Your Council Tax reference number (this can be found in the top left hand corner of your Council Tax statement)
- Your full postcode

Ready to start? Now visit [http://www.localauthorityname.gov.uk/eservices](http://www.localauthorityname.gov.uk/eservices) to activate and start using these new services. Further services are also planned and full details will be made available in due course.

The fact that the registration and enrolment process is powered by the Government Gateway is totally transparent to a user. Yet by setting up a user account in this way, not only do users have access to the local authority services, but also by default they gain a sign-on credential that provides access to all other public sector sites.

**Transactions**

A subsequent development beyond the use of single sign-on facilities is the use of the Gateway by a local authority for all of its transactions, as shown below.
At first glance, the above scenario may appear to offer a complex way of routing documents and interactions between a local authority and a user – after all, transactions now go via the Gateway rather than directly into the local authority system. However, from a wider e-government perspective, and from a user experience point of view, it has several strengths to recommend it. For example, a local authority can make use of existing infrastructure components, such as the secure messaging store, rather than constructing its own. It also enables a local authority to send an e-form onward to another public sector organisation (potentially such as a health trust, central government department or other local authority) using the Gateway’s organisation to organisation routing capabilities.

Although secure messaging is a single, central piece of infrastructure, its programmatic interface means that a local authority can present its content in a personalised way through its own local portal, using all its own branding and presentation. But since it is common infrastructure, the local authority can also make this view value-added, by enabling a user to view other items in the secure messaging system as well rather than just their dealings with the local authority.

Another key driver is that this second model also helps with joined-up transactions – for example, when a citizen moves from one local authority to another. By moving away from a model that is specific to one individual local authority to one that encompasses common infrastructure, it makes it possible for example to provide a user with a view of the final balance of their council tax where they used to live alongside a view of their new residence’s council tax.

Having common components is also important to independent software vendors and others who produce application software for local authorities and other government organisations. It means they can develop against a common set of consistent and standard interfaces, which will also facilitate the production of improved new versions of software that are e-government enabled.

**Inter-Organisation Messaging**

As mentioned in passing above, the Gateway also provides an infrastructure for authentication and messaging between organisations, such as between local authorities or between a local authority and a health trust. This is shown in simplified form below.
This inter-organisation messaging enables the common infrastructure to be used to move documents and communications between different government organisations – for example, a local authority could communicate with a central government department or a private pension company to make automatic electronic returns to say the DWP. Given the range of stakeholders and various parties that a local authority needs to communicate with, the Gateway provides a cost-effective and streamlined means of facilitating these connections and interactions.

As with externally-originated transactions, transactions between government organisations and related parties are also authenticated and automatically routed by the Gateway. The authentication and authorisation features of the Gateway ensure that all communication flows are fully authenticated and authorised during these inter-organisation information exchanges.

**Joined-up Transactions**

The Gateway also supports joined-up transactions. Rather than each connecting organisation merely replicating its existing paper-based forms, users can be offered a single form that integrates various existing paper processes into a more streamlined approach. This could be a consolidation of various information within a local authority, or to be shared between a local authority and other parties. A single consolidated form completed online by a user can then be de-composed into its component parts and each handled in accordance with existing processes. This is shown in overview in the diagram below.
A 10 step guide to getting online using the Government Gateway

**Background**

This section aims to answer the question ‘all this is very well, but what’s actually involved with getting services online using the Gateway?’ As is made clear elsewhere in this paper, the Gateway provides a key component in helping deliver against the government’s targets for making services available online.

Use of the Gateway’s e-government services will:

- save both time and money
- reduce the risk of launching successful e-services
- ensure that the Government’s overall joined-up vision is achieved.

The concept of the Gateway’s design is to ensure that its services are transparent to end-users, so that government organisations retain and strengthen their direct customer relationships through their own portals and web sites. Use of the common Gateway components – including authentication and authorisation, transaction handling, secure messaging and payments – mean that organisations can direct their resources into providing richer online services for their users rather than duplicating expenditure on existing infrastructure components.

**The 10 steps to e-service delivery**

The following steps provide a summary of how government organisations can take advantage of the common infrastructure offered by the Government Gateway to get their online services up and running as quickly and as efficiently as possible.

**Step 1- identify the services to be offered**

The first step involves identifying services to deliver online. These could range from simple processes, such as notification of faulty street-lighting by a member of the public to a local authority, through to the submission of a complex claims or benefits form.

For the services selected, decide what level of authentication each will require. The Gateway uses authentication standards based on the e-Envoy’s Authentication Framework:


Each service can have a security level of 0, 1, 2 or 3:

- level 0 – no security requirement (anonymous)
- level 1 – the service requires a user ID and password
- levels 2 and 3 – the service requires a digital certificate

If a citizen has a level 2 digital certificate, then they are able to enrol for all Level 1 and 2 services. If they have a user ID and password, then they are only able to enrol for Level 1 services.

The profile of users for the new service or services also needs to be decided. The Gateway supports three basic categories of user:

- individual (citizen)
- organization (business)
- agent (intermediary – someone acting on another’s behalf)
For the planned service(s), the organisation needs to decide which of these users the service is intended for (citizen or business) and whether those rights can be assigned to a third party (an agent).

**Step 2- identify rules and key information resources for the service**

For services that require authentication, decide on a set of information that will help to confirm the identity of a user. To enable the use of authentication and online services through the Gateway, a government organization needs to provide to the Gateway a database of identification information for each service they wish to implement. This contains a list of unique identifiers as well as some other qualifying information. This information is referred to as the set of “Known Facts”.

For example, Inland Revenue provides UTR (Unique Tax Reference), NINO (National Insurance Number) and postcode for their Self-Assessment tax service Known Facts database. In order to enrol for self-assessment, a user needs to provide their UTR and either of their NINO or postcode. Provided the information they enter matches a record in the Known Facts database, the user is then enrolled into that service, but the service is flagged as de-activated. An activation PIN to enable that account is then sent to the name and address that the department provides for that UTR.

The Known Facts databases are stored locally in the Gateway to ensure a rapid response time to user and programmatic interfaces. A related database of address information is also required, but this is always held inside the government organisation. When a user initially identifies themselves at the Gateway against the known facts during the process of enrolment to a service, it is this address that is used to mail out an activation PIN to enable that service. A set of services is able to share a single database if this is required.

The overall set of information that is needed to enable the Gateway to set up a service is:

- Known Facts and the rules that apply to them (eg. whether all or a combination of facts are required for a user to authenticate themselves in order to enrol into a service)
- the XML schema for the service
- the name of service
- the level of authentication required for the service
- the user profile for the service (citizen, business, agent)

There will also be the configuration information that needs to be jointly agreed to enable the Gateway and the organisation to communicate effectively.

**Step 3 - decide which Gateway components to use**

The Gateway offers several components:

- the authentication and authorisation service: this provides single sign-on across all government sites. It can be hosted within an organisation’s own web site or portal and be an integrated part of an organisation’s online environment
- the transaction engine: which authenticates and routes forms and other document submissions
- secure messaging: which provides the secure two-way communication facility between users and government organisations. This can be hosted within an organisation’s own web site or portal and be an integrated part of an organisation’s online environment
- payments: which provides both unauthenticated and authenticated direct debit, credit and debit card facilities. As with the other Gateway e-government components, this can be hosted within an organisation’s own web site or portal and be an integrated part of an organisation’s online environment
The organisation will need to decide whether it wants to use some or all of these services.

**Step 4 - develop, or re-use, a suitable form (XML schema)**

For the proposed service, details of the form or transaction and the underlying XML schema that defines it will need to be defined and agreed. Schema for online services are co-ordinated through the GovTalk group (see [www.govtalk.gov.uk](http://www.govtalk.gov.uk)). Depending on the service, there may already be a GovTalk schema that exists for a new service, or one may need to be designed from scratch.

**Step 5 - install and configure Gateway connection and integrate to existing systems**

In order for an organisation to interact reliably with the Gateway and exchange documents and forms, together with other data and exchanges (such as requests for addresses during the enrolment process), a dedicated connection is required. This is achieved through the use of the departmental integration service (or DIS). This provides reliable open-standards XML communication between the organisation and the Gateway together with a local integration facility that enables the XML to be integrated into existing information systems.

Various sizes of DIS are available depending on the anticipated volume of interactions. Once an appropriate model of DIS has been identified, it needs to be installed and configured inside the organisation’s chosen data centre. Depending on the configuration required, this may be a simple ‘black box’ installation, with minimal onsite configuration, or alternatively if full application integration to an existing system is required, may involve some customised work. As well as the DIS itself, the organisation will need to ensure the overall technical environment is suitably configured to handle the anticipated loads, performance and resilience required.

**Step 6 - build and test the application**

The application for the new service itself is of course required – either a desktop PC application, or one hosted online on a web site or portal. During development of this application, the e-government services from the Gateway can be used to accelerate development, reduce risk, time and cost – and also ensure that the delivered application is ‘joined-up’ and part of the wider e-government strategy.

To test the new service, sample data needs to be provided to the test Gateway. A DIS – or test DIS – service will need to be installed to enable full testing to happen since this is involved in the exchange of address request/response message pairs and other administration messages that pass between a connecting organisation and the Gateway.

Everything is now in place for the application to be built and tested. Use of the ISV test service and the test Gateway enable the application to be fine-tuned prior to launch. For the organisation, this step may also include hosting and testing the application within a web site, portal or PC application.

**Step 7 - prepare the Helpdesk and live services teams**

Any current helpdesk support in the organisation will need to be prepared to support the new service. Existing helpdesk tools can be enhanced by access to the Gateway’s helpdesk facility which provides helpdesk’s with a range of administration functions to help addresses callers’ problems – such as for example if they forget their user ID or password.

The team responsible for maintaining live systems will also need to be prepared for the launch of the service – from those who look after live web sites if that is where the new service is being hosted, through to those who look after the information systems that the DIS and other systems interface with. The same preparation will also be taking place at the Gateway.
**Step 8 - certify the application**
On completion, the new service will successfully pass testing and will then be certified as ready to go live.

**Step 9 - provide release data to the Gateway**
The live Gateway now needs to be loaded and updated with relevant information, such as the full known facts file.

**Step 10 - launch the service**
A date can now be agreed with the Office of the e-Envoy for the launch of the live service.

**Summary**
The Government Gateway provides a set of building blocks that expedite and simplify the processes of establishing online services. Making use of these components enables government organisations to direct their resources into the delivery of their own specific services in a cost-effective and timely manner, without replicating and duplicating common infrastructure that already exists.

The Gateway provides services that resolve the most complex parts of establishing online services –notably authentication, transaction handling, interconnectivity, secure communications and payments.
Gateway Features
This section looks at each of the main Gateway services in more detail.

Registration and Enrolment
Registering and enrolling are the processes involved with establishing users’ credentials and identity for use with government services. Users catered for include citizens, businesses and intermediaries (such as agents). The registration and enrolment system (referred to as R&E) provides the authentication and authorisation services that lie at the heart of enabling delivery of e-Government services in a joined-up, efficient and secure manner.

The incoming interfaces for users wishing to register and enrol for Gateway services use Internet protocols (HTTP, HTTPS) to support the required interaction with the consumers of these services:
- an end-user interface (client computers with browsers via the Internet)
- a programmatic interface (programmatic interactions via the Internet using web services – enabling web sites, portals and desktop application software to interact directly with the Gateway)

A service can consist of one or more transactions. A "transaction" is in reality an XML message that can be used to either submit or request information. Each service has an associated security level of 0, 1, 2 or 3. These security levels are defined in the Office of the e-Envoy's Authentication Framework (http://www.e-envoy.gov.uk/publications/frameworks/authentication/authentication.htm).

Level 0 means that there is no security requirement, level 1 means that the service requires a User ID and password, levels 2 and 3 mean that the service requires a digital certificate. If a citizen has a level 2 digital certificate, then they are able to enrol for all Level 1 and 2 services. If they have a User ID and password, then they are only able to enrol for Level 1 services.

Known Facts
The Known Facts database underpins the Gateway’s registration and enrolment service. To enable online services through the Gateway, a government organisation provides to the Gateway a database of identification information for each service they wish to implement. This is referred to as the Known Facts database and contains a list of unique identifiers as well as some other qualifying information.

For example, Inland Revenue provides UTR (Unique Tax Reference), NINO (National Insurance Number) and postcode for its Self-Assessment tax service Known Facts. In order to enrol for self-assessment, a user needs to provide their UTR and either of their NINO or postcode. Provided the information they enter matches a record in the Known Facts database, the user is then enrolled into that service, but the service is flagged as deactivated. An activation PIN is then sent to the name and address that the department holds for that UTR.

The Known Facts databases are stored locally in the Gateway to ensure a rapid response to both the user and programmatic interfaces. The address information however is not stored in the Gateway. This is instead provided as a result of a request/response interaction between the Gateway and the government organisation concerned. A set of services is able to share a single set of Known Facts if this is required.

Supported Types of User
The Gateway supports three basic categories of user:
- individual (citizen)
organisation (business)
agent (intermediary – someone acting on another’s behalf)

Individual (Citizen)
Individual users represent themselves directly on the Gateway and this category is the most common type used by citizens. Individual users are able to:

- enrol for all individual services
- choose and change passwords (if using User ID/Password)
- change their details (name if not a certificate user and email address)
- de-enrol from any services already enrolled for
- de-register from the Gateway (which effectively de-enrols them from all enrolled services and removes their account from the Gateway)
- upgrade their credential from a User ID/Password to a certificate
- nominate an agent for some or all services for which they are already enrolled

Organisation (Business)
The organisation category provides a more flexible model, suitable for use by businesses. The Gateway provides the ability for an organisation to have more than one user associated with an account to reflect the fact that an organisation will probably want more than one employee with access and for them to undertake a range of tasks. The organisation category supports two types of user.

- **Standard user**: these users have full control over all functions in an organisational account in the same way as if they were a standard individual user. Any number of users may enrol in the service so that, for example, all members of a payroll department could use the service (without sharing the account – each would have their own credential). Each standard user account is equal in rights and status. A new user can only be added by being brought into the account by an existing user (so the first user has to bring in the second, but after that either user can bring in more users, and so on). Initially, a new user brought into the account will only be a level 1 user (User ID and password). This is because the new user may not be present at the time and if a certificate were to be used they would not be able to sign at the time. That new user can then upgrade their credential to use a certificate if they need to in order to use the services available.

When standard users are added into an organisation they will not automatically be assigned to any of those services. The process of associating users with the various services is called mapping. So, for example, an organisation would wish its payroll users to be mapped to PAYE services, but not to VAT. Other users within the organisation would then be mapped to the VAT service. In this way, the Gateway supports the roles and responsibilities within an organisation and allows them to be reflected in the Gateway in terms of who has the rights to act on behalf of the organisation across the various available services.

- **Assistant**: these users have far more restricted rights than standard users. A user is able to create an assistant and is then responsible for the actions of that assistant. An assistant can only:
  - Log in to the Gateway and change their details (password, email and name)
  - Upgrade their credential to a certificate
  - Carry out those specific services to which their parent user has given them permission

An assistant can only be mapped to some or all of the services to which the parent user is mapped. An assistant is unable to create assistants, delete any other assistants or change the mappings of other users. If a user with one or more assistants is removed from the Gateway, the assistants are not deleted but are disabled until another user ‘adopts’ those assistants.
Agents (Intermediaries)

An agent is able to do everything that an organisation is able to do, but can only register for agent class services. These services do not actually allow the agent to do anything, but a client (an individual or organisation) is unable to allocate any of their services until an agent is enrolled for the appropriate receiving service. For example, an agent may enrol for the Inland Revenue Self-Assessment agent service. This will not initially allow them to submit any SA returns. However, an individual class user is then able to allocate that agent to their SA service. Once allocated, the agent is then able to submit SA returns on behalf of that individual class user.

Registration

Registration is the process of creating a user account and either:

- setting up a User ID/password. When a user registers in this way they will be asked to enter the following information:
  - their name (no validation is carried out on this entry)
  - their email address (optional if they want to receive email notifications of submissions and secure messages).
  - a password (meeting the following rules)
    - be between 8 and 12 characters (letters and numbers)
    - contain at least one number (0-9)
    - contain at least one letter (A-Z or a-z)
    - not be, or contain, the word "password"
  - the user will then be asked to enrol for one or more services (see next section for details) and if successful will be presented with their User ID. Their User ID will also be sent to them as a reminder through our secure mail process (the second reason for forcing one enrolment is to ensure we can get a suitable address to send the user id to as a reminder)

- recording details of a user’s t-scheme digital certificate. They will be asked for the following:
  - their name. However the name is taken from the X509 certificate and cannot be altered or changed
  - their email address (optional if they want to receive email notifications of submissions and secure messages)
  - the certificate is checked against the appropriate CRL to ensure it is valid and the signature is checked to ensure that the contents have not been altered and to provide non-repudiation

The service that is being enrolled for will dictate the level of authentication required (i.e. no authentication, User ID/password or digital certificate). Users can register as an individual, organisation or agent.

Users will need to register once to use the Government Gateway, and then will enrol for each specific service that they wish to use. At the time of registration, the user must enrol into at least one service. Failure to enrol for a service will mean the account will be deleted.

Gateway Home Page UI

This is the initial page that users see at www.gateway.gov.uk. It provides a variety of background information about the services available, the Gateway itself and links to background information.
Gateway Registration Page
This page enables users to choose which type of registration to select – individual citizen, organisation or agent.
Citizen Registration Pages
The initial citizen registration page provides an overview of the process involved. It also allows the user to choose whether to register with a User ID or with a digital certificate.
The next page then asks for some basic personal details, which the user completes (including optionally their email address).

**Enrolment**

A list of currently available services will then be displayed. The user will select those in which they are interested and then click the continue button in order to enrol in them. For each of the services selected, the user will then be presented with a screen to enter the personal data that will identify them to the government organisation concerned.

Provided the user has correctly entered the details, they will then be matched against the Gateway’s copy of known facts and the user successfully enrolled on the Gateway. They will receive notification screen indicating success or failure and the fact that they will be sent an activation PIN within the next 7 days. Where users have also opted to enter their email address, confirmation email will also be sent along the lines of the following:
Thank you for enrolling for the Internet Service for Self Assessment service through the Government Gateway.

We will issue an Activation PIN for this service within 3 days, so you should receive it through the post within 7 days. If you have registered on behalf of an organisation, the letter containing the Activation PIN will be sent to the contact name and address to which paper forms and other correspondence for this service are normally addressed. In this letter, the contact will be asked to give the Activation PIN to you providing that your organisation has authorised you to use this service on its behalf.

Once you have received the Activation PIN you will be able to activate the service. You will then be set up ready to send forms over the Internet for this service.

If you have not received a letter from us within 7 days, please contact the Internet Service for Self Assessment Helpdesk on 0845 60 55 999.

To find out more about the Internet Service for Self Assessment service, including how to send your forms over the Internet, please visit www.inlandrevenue.gov.uk/e-tax/index.htm.

About the Government Gateway

The Government Gateway is the centralised registration service for e-Government services in the UK. For further information about the Government Gateway, please see the Government Gateway website at www.gateway.gov.uk.

Thank you for using the Government Gateway.

Enrolment

Each Gateway service represents a collection of business services (such as transactions) appropriate to a specific community. For example, a Local Authority could choose to allow a citizen to enrol for its “Housing Services”. A single enrolment to “Housing Services” could give the citizen access to both Council Tax and Housing Benefits transactions.

For each service, the user is asked to enter some known facts. Known facts are verified within the Gateway to ensure that they are accurate. Organisations are expected to supply known facts data to the Gateway, plus provide timely updates to this data.

Also associated with each service is the authentication level required to use that service. Users who authenticate themselves at level 1 (User ID and password) do not have access to services specified as requiring level 2 authentication. Users who have a level 2 digital certificate do however, have access to level 1 services.

Once enrolled in a service, once logged in to the Gateway the user will see a list of their services.
Assigning Agents

Agents are appointed at the service level: this means that a registered user can appoint different agents for different services and retain some services to handle themselves. To assign an agent for a service, the user selects the ‘Add Agent’ option on the screen. They are then presented with a screen where they can enter the agent’s identifier in order to assign the agent to that service.

Activation

Activation PINs are used to ensure the user is who they claim to be (and that they are authorised to perform transactions on behalf of the organisation they represent if they are representing a business). They are used just once.

When a user enrolls for a service, a message is sent to the appropriate organisation (such as a Government department or a local authority) requesting the name and address associated with the Known Facts matched by that user. An Activation PIN is then printed at a secure print facility and sent to the name and address provided by that organisation to the Gateway. The user will receive their activation PIN within 2 – 7 days. They then enter the activation PIN. This completes the enrolment process for that service. This process is repeated for each service the user enrolls into.
The user must activate their enrolment by presenting their PIN, either to the Gateway directly or via a suitable portal, within 28 days. After a period of 28 days has elapsed the original PIN will be rejected but the user’s credential is kept. Where a new PIN is requested a further 28 days will be granted.

If a user incorrectly enters their activation PIN three times in succession, then the enrolment is removed. Please also see ‘department activation token’ (below) for an alternative approach.

**Department Activation Token (DAT)**

A DAT enables a government organisation to mail-shot potential users in advance of the normal process so that users can begin to use their services immediately upon registration and enrolment. The user registers as usual but at registration time users have their DAT checked in the same manner as other known facts. The Gateway recognises that one of the known facts is a DAT and, if successfully supplied, automatically activates the new user.

DATs are generated by the government organisation and the responsibility for expiring them remains with the organisation.

---

**Gateway Services, including Level 0 Services**

The Gateway defines a service as a group of associated business submissions that all have the same destination and authentication requirements. For many services, the Gateway receives business transactions where the user is required to supply level 1 or 2 credentials.
within the submission that are then validated as current Gateway credentials. These credentials can be a User ID and password or a digital certificate. This follows the accepted t-scheme levels as laid down in the UK Government document titled ‘Authentication Framework for Information Age Government’:

- **Level 0**: no authentication required
- **Level 1**: authentication required to protect against minor inconvenience or loss (User ID and password)
- **Level 2**: authentication required to protect against significant inconvenience or loss (digital certificate)
- **Level 3**: authentication required to protect personal safety and/or to prevent substantial financial loss

As well as the authenticated services, the Gateway supports submissions from an unregistered Gateway user. This type of service is described as a ‘Level Zero’ service.

Level zero services allow users to submit business documents through to a Government department or organisation without any registered credentials – for those services that explicitly permit this. Level 0 supports those services where no authentication is required (for example a request for information from a department).

**Registration and Enrolment – User Interface**

**Generic Process**
The basic registration process is:

- a user selects the type of registration they require (individual, organisation, agent)
- the user selects the type of credential they wish to use (certificate or User ID/password)
- for User ID/Password the user enters full name, e-mail address and password
- for Digital Certificate the user selects the digital certificate they wish to use
- the user selects the service(s) they wish to enrol for (at least one is mandatory at registration)
- the user enters the known facts they wish to use for each enrolment (service)
- the known facts are validated against service specific known facts held on the Gateway
- when valid the user is thanked for their interest and informed they will receive notification through Royal Mail of their User ID, which is also displayed to them then and there on the screen

The remaining processing of the registration takes place asynchronously:

- the known facts are sent to the government organisation that owns the service
- the organisation validates the known facts and sends the postal address associated with those known facts back to the Gateway
- the Gateway sends, via Royal Mail, a letter to the postal address provided by the government organisation. This contains a one-time activation PIN for digital certificate registrations and a generated user id for User ID and password registrations
- the user receives their Royal Mail letter
- the user returns to the Gateway (or the appropriate portal) and activates their registration by entering the one-time activation PIN, or using their User ID/Password for the first time.

Once registered, a user can enrol for other services. This process is similar to that used for initial registration. Each new service added is associated with the same initial credential (User ID/Password or certificate) so that the user has a single identifier to use across all the services for which they enrol.

The Gateway stores enrolment known fact identifiers against user credentials and whenever the Gateway passes a message to a government organisation, it adds the known fact
identifiers to the message enabling the organisation to process the message appropriately. To conform to data privacy rules, the Gateway does not reveal to government organisations the known facts provided for enrolment to other services.

Each service is composed of one or more classes. Each class represents a function that enrolled users are permitted to perform via the Gateway, e.g. submit an end of year tax return.

**Citizen**
Before an individual can use services which exploit the Government Gateway’s authentication and authorisation features they must register and enrol. A citizen registers once with the Gateway (or via a web site using the Gateway’s programmatic facilities) to obtain single credentials for logon that they can then use across all government web sites and services. This will either be a User ID and password or a third party digital certificate. They then need to enrol for each service that they wish to use. A service can include one or more transaction types. Each service identifies a set of related end user facilities, e.g. Company Tax Returns, Local Authority services, Agricultural Farmers.

During registration the user must enrol with at least one service. The user enters general details about themselves and separately enters specific details (known facts) relating to each service for which they wish to enrol. The service specific details for each enrolment are sent to the government organisation that provides the service for verification. When valid, a postal address is returned to the Gateway and is used to send a one-time activation PIN for the service to the end user. The user activates their enrolment by entering the one-time activation PIN (either on the Gateway or an appropriate portal) the first time they attempt to use the service.

Users of the Gateway are able to login to the Gateway to perform account management activities such as nominating an agent who will act on their behalf.

Registration and enrolment also allows for users to be pre-enrolled on the Gateway. This enables government organisations to pre-send an activation token (called a Department Activation Token or DAT) to their customers by post to expedite their enrolment on the Gateway. This enables users to come to a government organisation web site or the Gateway itself and complete the registration and enrolment process in its entirety there and then (without incurring a time lag while waiting to receive their activation PIN in the post). The user enters their Known Facts and their DAT to enrol for a service. As soon as this process is successfully completed, they are able to use the associated online services immediately.

**Organisation**
A similar process applies to businesses as for citizens, but a more flexible model is provided which reflects the need to support delegated responsibilities. To avoid the need for credential sharing within organisations, the concept of a Credential User Group (CRUG) is supported.

Each user who registers with the Gateway is automatically placed within a CRUG and their enrolment details (known facts) are held at the CRUG level. A user within a CRUG has access to a range of facilities that enable new users and new assistants to be added to the CRUG. When creating a new user or assistant, the services they are permitted to use as a member of the CRUG are specified as part of the creation process. All users within a CRUG are able to create new users and pass on access to the services they have access to. Assistants do not have access to the facilities that enable new users or assistants to be created.

All members of a CRUG share a common set of known facts for the services that they share. New members of a CRUG are created by an existing user requesting the generation of a level 1 (User ID/Password) for the new user or assistant. New users or assistants may then come to the Gateway and use the User ID/Password in the usual way. They may also upgrade their user credential to a digital certificate if level 2 access is required.
Agent
An agent is someone (individual or organisation) that represents another legal entity (such as a citizen or business). As such they are unable to carry out any services on behalf of another entity until they are given permission to do so by that entity. An example of an agent may be an accountant, a payroll bureaux or someone with the power of attorney over another.

Registration and Enrolment Web Services
The previous section outlined the registration and enrolment facilities, and used some screen shots of the Gateway’s own user interface. However, the Gateway also exposes many of its authentication and authorisation functions as a web service. This enables portals to provide a range of facilities within their own web sites – such as registering a user for a single Government credential, or using single sign-on facilities – without the user needing to be aware of the Gateway. The portal is able to interact programmatically with the Gateway and make use of its services, improving the user experience and enabling the portal to leverage the common infrastructure components of the Gateway in a flexible and useful way.

Note that the Gateway persists no state for the user session: that must all be handled within the portal. Gateway credentials form the basis of authentication within a portal. The portal’s local authentication manager will not hold its own authentication database. Personalisation and other customisable features specific to a user or group of users can still be achieved in the portal since the Gateway always returns a unique user identifier that the portal can map to personalisation features.

Using the Gateway’s web services, the portal is able to hide the complexity of authentication, i.e. the user will not have to browse to the Gateway to register and enrol. This will be handled by the portal, which can present its own UI to the user and then broker the interactions with the Gateway using the web services. The portal can also decide whether to allow an e-applicant to choose whether to enrol or not when making an unauthenticated submission. Anonymous business form submissions may be allowed on a per-service basis. In other words, unauthenticated or not-logged-in users can enter the portal, optionally browse information and go on to full business form submission.

The core R&E services exposed programmatically by the Gateway as web services are:

Register a new user
This allows the portal, external system or any suitable client to register a new user on the Gateway and at the same time enrol them for their first Gateway service. If the registration and enrolment is successful, the caller is returned a service ticket to present in subsequent calls to Authentication along with essential Gateway user information like the User ID and credential identifier.

Enrol a user for a service
This method allows the portal to enrol a registered user for a Gateway service. If the enrolment operation is successful, the caller is returned a modified service ticket to present in subsequent calls to Authentication.

Log a user on
This allows the portal to effect a user logon, using the Gateway as the authentication source. If the authenticate operation is successful, the caller is returned a service ticket to present in subsequent calls to Authentication.

Log a user off
This just releases the service ticket obtained by earlier calls to the above methods.

Activate a Service
This allows the portal to activate a user who has been enrolled in a service and has now received their activation key through the post.
De-enrol a User from a Service
This allows the portal to de-enrol a registered user from a Gateway service. This is possible only for logged-in users.

Get a Login Document
Provided for digital certificate users, this method prepares for a certificate-based login. Digital signing of a Login Document is used to verify that a user owns a digital certificate and hence allows them to log in as the entity described in that certificate.

Change Password and User Details
These methods enable changing a level 1 user password, or user details in general. The user must be authenticated before this method is used, in the same way as the old password is always requested on standard password-change screens.

Agent Assignment
Matching Existing Agent to new Principal
R&E enables a newly enrolling principal’s identifiers to be looked up to check whether they are already represented on the Gateway by an agent. This occurs only during registration.

The process followed is:
- When the principal enrols, the service identifiers are looked up against existing agent identifier groups for the same service.
- If matches are found, look for one that doesn’t currently have a registered principal associated with it.
- If a single match is found, no new identifier group ID is allocated, the principal’s identifier group becomes the existing one identified by the match.
- In cases where zero or several matches are found, no further action is taken.
- Assuming a single match and a successful setting of identifier group, the UI enables the user to immediately see the association with the agent once registered.
- The above functionality happens if the user is auto-enrolled via a department.

This facility works on the basis that any given set of service identifiers is unique in the whole of R&E.

Agent De-Allocation
During the process of de-allocating an agent, all principals affected by the agent removal or de-enrolment are located. Affected Gateway-registered principals are then set so they are responsible for their own service, while non-registered principals are removed.

Messages are then sent to the affected department(s) as follows:
- An enrolment notification message providing the agent ID who has un-enrolled or been de-enrolled by the back end.
- An agent rights notification message in respect of all principals affected, with their unique service identifiers.

The following points must be noted about these messages:
- The two messages may arrive in any order
- They do not share a common correlation ID
- The agent rights notification message will likely contain multiple <Allocation> blocks which the department must be able to process.

It is a government organisation’s responsibility to take appropriate action according to their individual services. Such actions could involve contacting the principals involved so that re-assignments or un-enrolments can be agreed and consequently applied. This is particularly important in the case of a principal who is not registered on the Gateway because they had assigned the agent by paper means.
**Auto-Mapping an Agent**

R&E provides a facility for automatic mapping of a single agent:

- A principal assigns an agent for a service via the R&E UI or an agent rights allocation message is received from the department.
- R&E checks the agent users in the agent group.
- If there is a single agent, an automatic mapping is made so that the single agent user does not have to map to the principal manually (the agent sees the association in the R&E UI automatically).

If there are other agents in the credential group, no automatic mapping is done.

**Administration Functions**

The Gateway also provides a range of administration functions for interactions between government organisations and the Gateway. These comprise both government organisation initiated functions and Gateway-initiated functions.

**Government Organisation Administration Services**

The business services supported in this way are:

- **Reset Password**: re-sets a user password and the user is notified of the new password via a Royal Mail letter
- **Un-enrolment Request**: removes a user from a service
- **(De)Allocate Agent**: causes an agent to be allocated or de-allocated to act on behalf of another user
- **Address Response**: provides a postal address relating to a set of known fact identifiers to the Registration and Enrolment process (returned in response to an address request generated and sent to the government organisation as part of the enrolment process)
- **Known Fact Updates**: causes a series of updates (additions, modifications and deletions) to be applied to the known facts held for a particular service

**Gateway-initiated Administration Notifications**

Registration and Enrolment generates a number of administration requests and notifications to departments. The business notifications and requests are:

- **Address Request**: generated by on-line activity within one of the registration user services to obtain the postal address held by the government organisation for a set of known facts entered during the enrolment process
- **(de) enrolment notification**: generated by on-line activity within one of the registration user services and notifies the organisation that someone has revoked their enrolment to a service
- **(de) agent notification**: generated by on-line activity within one of the agent user services and notifies the government organisation that a user has allocated or de-allocated an agent to act on their behalf

**Transactions**

The functions of the Transaction Engine are:

- to authenticate and route transactions between citizens and government organisations
- to authenticate and route transactions between businesses and government organisations
- to authenticate and route transactions between government organisations

As well as a standard Internet interface where documents can be submitted (via a public URL), the Gateway also implements a hub and spoke model. In this model the hub is the
Gateway and the spokes are government departments, local authorities or other public sector or related organisations. All spokes are able to submit business transactions directly to the Gateway and have the responses delivered directly to their spoke. Spokes are also able to receive business transactions posted into the Gateway and destined for them.

**XML Submissions**

The Transaction Engine is designed to use XML both inbound and outbound, in line with the e-GIF. However, not all browsers implement the World Wide Web Consortium (W3C) recommended XML specification. The lack of full native XML support would reduce the ability of some applications to submit data to the gateway and receive an XML response. With this in mind, the Gateway also provides support for XML to be submitted via the Hypertext Markup Language (HTML) standard.

Although the HTML implementation reduces the purity of the Government Gateway, as it dilutes the design of XML-in / XML-out, it does enable non-standards browsers to be supported.

The Gateway therefore implements two ways of submitting data:

- Pure XML
- Base64 encoded XML in a HTML tag

**Functions**

In terms of the main functions of the Transaction Engine, these can be summarised as:

- adding a timestamp
- adding a Transaction ID
- adding an audit ID
- adding a Correlation ID
- checking and storing of any return routing information
- calling the R&E Engine for Authentication and Authorisation
- parsing the XML Header
- parsing the XML Body
- forwarding the transaction to its destination
- forwarding messages to the user/submitter
- where appropriate, routing any return message to the destination point indicated in the stored routing information table for that particular transaction

**Citizen and Business Submissions**

The Gateway is an XML-in/XML-out engine and uses XML schema defined by GovTalk. All XML is based on the W3C XSD standard. 128bit SSL is used to protect the XML as it passes across the Internet.

In a typical usage scenario, the user (whether citizen or business) will log on to a departmental Web site hosting an electronic form application, or make use of an application resident on their PC. The user then completes an electronic form either via a hosted application or a local application.

In the case of a hosted application there are two scenarios:

- either the completed form is downloaded to the user’s PC for signing, or
- an application is downloaded to the user’s PC

In either case the authenticated form is then electronically posted to the Gateway.

The Gateway authenticates the message and confirms the user’s authorisation. Globally unique identifiers and a time stamp are attached to the transaction. The form’s XML Header and Body are then parsed before the document is forwarded to the appropriate destination.
When the destination organisation’s delivery point has carried out any required functions, the transaction is then forwarded to their systems for processing. On completion of this a message is forwarded back to the waiting user to confirm acceptance or rejection of the transaction.

The user would typically save this response, as it is a legal document. In the case of a successful submission it constitutes definitive proof of delivery.

**Business to Government Organisation communication**

Businesses have several ways in which they can submit business forms and documents:

- directly from a Gateway-enabled business application: instead of printing out and submitting forms manually, Gateway-enabled applications can instead submit submissions (such as VAT and PAYE returns) directly over the Internet
- via a suitable portal: various government portals provide the means to complete and submit business forms on-line
- as a dedicated spoke: this is a suitable approach for those businesses engaging more frequently in interactions with government or in additional volumes, such as pensions providers. It enables businesses to have an always-on, two-way communication link with government and other related organisations. Not only does this mean documents can be submitted as and when the need arises, as with the above methods, but also that responses and other documents being received can be received in real time and integrated into the businesses existing systems

**Citizen to Government Organisation communication**

Citizens have several ways in which they can submit forms and documents:

- directly from a Gateway-enabled application: instead of printing out and submitting forms manually, Gateway-enabled applications can instead submit submissions (such as Inland Revenue’s Self-Assessment return) directly over the Internet
- via a suitable portal: various government portals are providing the means to complete and submit forms on-line (including Inland Revenue’s Self-Assessment online service)

**Government Organisation to Government Organisation communication**

Government organisations will generally use the dedicated spoke approach. This enables government organisations to have an always-on, two-way communication link with the Government Gateway. It therefore enables both the two-way interaction with businesses and citizens, as well as with other government organisations. Not only does this mean documents can be submitted as and when the need arises but also that responses and other documents can be received in real time and integrated into an organisation’s existing systems

**Internet Polling**

After a submission over the Internet, clients can poll the Gateway for a response. This will indicate the success or failure of their submission. In the case of failure, details will be provided of why the submission failed.

Polling is not required by spokes since they will automatically receive responses via their Gateway connection.

**Government Organisation Integration**

As mentioned above, Government organisations operate in an always-connected mode making use of the Gateway’s hub and spoke design. The Gateway currently provides this link via a service known as the departmental integration service or DIS for short.
DIS is a suite of hardware and software that can range from a single server through to a highly available clustered server installation. By default, it provides full support for the GovTalk XML schema used by the Gateway together with additional features to ease integration such as automated digital signing of administration messages.

DIS provides communications between the Gateway and the participating government organisations. It also offers the option of integration between the XML required by the Gateway and the local data format needs of the organisations’ systems. DIS is able to map from XML to a wide variety of data formats, identifying a matrix of mappings of the relevant XML schema to the back-end organisation’s data-specific interface requirements. This mapping enables DIS to simplify the integration of application data between the Gateway and the organisations’ local systems. Data ranging from key extract information, which the government organisations need to supply to the Gateway in order for users of the system to be authenticated, to the exchange of business specific forms can all be passed through the Gateway and will all be treated in the same way.

An example flow of data through DIS is as follows:

- DIS receives an XML message from the Gateway that conforms to the appropriate GovTalk schema for that particular type of transaction
- DIS passes the XML message onto that organisation’s local server for processing
- The organisation’s local server processes the message and, where appropriate, sends a response back to DIS
- DIS routes the XML response back to the Gateway for final processing and correlation with the original message

This data flow is illustrated below, with the additional option indicated of the DIS undertaking a transformation to the local data format required.

**Note:** Specific DIS to organisation interfaces and data exchanges must be developed on an organisation to organisation basis as each organisation comes on-line with the Gateway, to ensure these interfaces meet each organisation’s specific technical needs.

DIS uses shared queues for processing and exchanging documents, which ensures that documents are never lost or deleted. When a document is set on the queue, the first available server retrieves and processes it. If a document is not successfully sent via the secondary protocol, DIS places the document into a dead letter queue. By periodically replicating the shared queues for a group on other servers, DIS creates a primary and secondary database. This replication allows users to take servers offline, or to add new servers without forcing stoppage of the entire system or losing track of documents.
Delivery Mechanisms
DIS uses HTTP Post to deliver documents to the owning organisation and to the Gateway. DIS receives administration documents from the organisation via HTTP Post. DIS receives Known Facts Extracts (full and update) via FTP or HTTP from government organisations. These are delivered to a known location on the Gateway.

Reliable Messaging
Reliable Messaging between DIS and Gateway is implemented. When a document is sent between DIS and the Gateway one of the following events must happen:

- The document is delivered exactly once
- The document is not delivered and the source server is notified that delivery failed.

Reliable messaging between an organisation and the DIS itself is provided in accordance with the Gateway Protocol both synchronously and asynchronously.

Security
DIS is able to sign outgoing business and admin messages with its own Gateway recognised certificate. This is a Gateway requirement but also enables government organisations to operate their DIS on the Gateway as an Internet-enabled spoke if they so wish. DIS secures its traffic using SSL client-certs or VPN thus ensuring received traffic is from the Gateway and the transport is secured.

Flow Control Component
There is an optional Flow Control component supplied with the DIS software, which allows an organisation to instruct the DIS to stop sending messages. The messages are held on the DIS and can be released later via another instruction. The flow control component provides the following functionality:

- monitors the Suspended queue and reacts to Suspended queue events that are raised
- automatically stops the flow of messages to an organisation if a document, which is not recorded in the resend-entries table, reaches the Suspended queue with a transmission failure reason code.
- automatically resends a message to an organisation if a document, which is recorded in the resend-entries table, reaches the Suspended queue with a transmission failure reason code.
- provides support for the flow control start and stop functions to set or reset the appropriate database table entry.
- creates and sends an e-mail to the nominated administrator when the flow is automatically stopped, using the SMTP service. The e-mail addresses and subject line are taken from the registry
- raises an SNMP event trap when the flow is automatically stopped, using the DIS SNMP component. The event code to be used is read from the registry.
- raises events which allow a client monitor program to monitor the operation of the Suspended queue, if required.

Auditing
In addition to standard Windows event logging DIS provides an audit capability which logs events to a DIS specific database. Audit entries are written by DIS in the following circumstances:
Receipt of an incoming document from the Gateway.

Receipt of an incoming document from the department back-end system.

Receipt of an incoming Known Facts documents from the department back-end system via FTP.

Successful transmission of a document to the back-end system

Failed attempt to transmit a document to the back-end system

Department responded with a Resend request (a recoverable error response) to the transmission of a document to the back-end system.

Flow control service has automatically stopped the flow of documents to the back-end system.

The flow control service has restarted the flow of documents to the back-end system on request by the user.

The flow control service has stopped the flow of documents to the back-end system on request by the user.

Other Key Features

Some of the specific features of DIS include:

- **Provisioning**: users can configure the DIS, remotely if required, to change configuration or add new services. Some examples, but not exhaustive, of configuration changes available under this means include: changing where documents are sent, changing conversion formats, or adding entire new services. All this functionality is achieved via sending a correctly formatted XML document to the DIS

- **Remote Monitoring**: users can examine the length of the work queues via a web browser and check the status of services. Services may also be securely start/stopped via this means

- **Diagnostic Tracing**: through the use use of web log files and custom diagnostic files

- **Installation Process**: DIS Installation and un-installation is much simpler, using an MSI-based InstallShield program. The installation program allows for a range of DIS installs from clusters to laptops. Clean un-installs are similarly provided for

- **Integrated Test Tools**: users can use an automated test tool, not only to regression test the DIS, but also to help new sites verify that their back-ends can integrate correctly with the Gateway

- **Internationalisation**: DIS supports documents in any language, including for example Japanese, Greek and Welsh

- **Optional Document Validation**: optionally users can now validate incoming documents’ format and size before they are accepted. Where applied invalid documents are rejected back to the originator at the point the originator submits them

- **GovTalk version Transformations**: optionally, DIS now provides translation between old and new GovTalk header formats

- **Message Signing**: as part of the ‘hub and spoke’ model DIS supports PKI signing of messages. This greatly improves security by for instance, ensuring that only messages signed for by the owning and/or permitted user will be acted upon by the Gateway
- Alert notifications: DIS can raise alerts via both SNMP and SMTP to designated content points if the delivery of messages from DIS to an organisation is halted for any reason.
Additional Gateway Features

Secure Messaging

Secure Messaging provides a secure two-way communication channel between Gateway users and government organisations. All users that register on the Gateway automatically receive a secure mailbox. At this point a standard ‘welcome’ message is always deposited in the new user’s mailbox.

User-Initiated Communication

Messages can be initiated by users and can be composed:

- directly on a user interface provided by the Gateway secure output facility
- on a user interface provided on portals/applications which then use a SOAP interface into the Gateway secure messaging system

Details of the SOAP interface and associated XML schema can be found at http://www.govtalk.gov.uk/.

Once completed, the resulting messages are posted through to the relevant organisation. Users are only able to communicate with those organisations and for those services for which they are enrolled.

When received by a department or other government organisation, messages can be distributed internally via any method the department chooses. For example, an organisation might choose to map between the XML message received and an internal SMTP-based mail system internally.

Government Organisation-Initiated Communication

Messages from government organisations to users are XML messages that are returned to the secure messaging system. There are several options the organisation can choose to use:

- whether the user is allowed to reply to the message or not
- whether if a message is not read by the expiry date set then it is to be sent back to organisation to take appropriate action. The message itself is not deleted.
- whether the message should go to agents, to the users they represent or both

View Inbox
Create New Mail

Users are able to create and send new mail to a set of destinations appropriate for those services for which they are enrolled. As with many secure messaging systems in use with financial institutions for online banking, users can choose their topic and enter lines of text raising issues or responding to points in previous communications.
In the example below, the user has selected the Internet Self-Assessment Service and decides to raise issues about the tax statement which has previously arrived in their secure messaging area.
Sent Messages
The secure messaging service also enables users to view messages they have sent as well as those they have received.

Notifications of new secure messages
Under Mailbox Options, users can elect, if they wish, to be notified via email when new messages arrive in their secure messaging area. The email will not itself contain the contents of the message – to ensure that nothing confidential passes over the Internet – but will merely let the user know that there is a new message that they should come to view within the secure messaging area.

It is planned over time to enhance this notification service to provide users with a wider choice, which will encompass the likes of instant messaging clients, mobile phone text services and so on.
Helpdesk

The Helpdesk facility provides a range of functions for departmental and other connected organisations’ helpdesks.

Payments

The payments engine provides support for both authenticated and unauthenticated payments. It includes support for debit cards, credit cards and direct debits.

Please contact the Office of the e-Envoy for latest information as to when this service will launch.
Appendix A – Standards

The Gateway adheres to the UK Government’s e-GIF (electronic-Government Interoperability Framework), which commits it to track and implement W3C/IETF and other open standards. Details on this standard can be found online at http://www.citu.gov.uk/e-gif.html.

The Gateway accepts and generates Extensible Markup Language (XML), a meta-markup language that provides a format for describing structured data within electronic documents. A schema can be attached to an XML document. Schemas specify the structure of an XML document and place constraints on its content. While XML is the meta-language that defines the rules for defining tag languages, a schema can be thought of as the formal specification of the grammar for one tag language. XML is defined by the World Wide Web Consortium (W3C), ensuring that structured data will be uniform and independent of applications or vendors. Further details on the XML standard can be found at http://www.w3.org.

All XML files submitted to or output by the Gateway must conform to a pre-set schema known as the GovTalk schema. The GovTalk schema is the formal specification of the elements and attributes that are allowed within a particular class of document, how those elements and attributes are related to each other and the sequence in which they must appear. More details are available online at the UK Government GovTalk official site at http://www.govtalk.gov.uk.

Appendix B – Developer Information

There is a support site provided for developers wishing to make use of the Gateway. It is called Gateway Partnerlink. The URL for this site is www.govtalk.gov.uk/gateway_partnerlink. It can also be accessed through the home page on GovTalk.

The aim of this site is to provide information to Independent Software Vendors (ISVs), Departments and Local Authorities about the Government Gateway.

Highlights of the site include:

- information for ISVs on how to develop Gateway enabled products
- detailed information about Gateway components
- a partner directory which contains details of some of the Government Gateway partners that OeE has worked with. However if you are an ISV and would like to be added, then please complete the template on the site
- the ability to subscribe to a monthly newsletter for Gateway news
- a projects directory that describes projects that use the Gateway
Appendix C – Potential Future Enhancements

The Gateway continues to enhance and develop additional functionality and services. The following, which is subject to change, provides an indication of potential future updates.

Release 1.6

- Auto-enrolment
- Multiple enrols to a service, with different identifiers
- UI checkbox for T’s and C’s
- Rules change for validation of company registration number
- Agent assignment
- Various CR’s
- Payments
  - Direct debits, credit cards, debit cards – through web service
- Business submissions via DIS + DIS cert mgt
- Helpdesk User ID resend facility

Beyond 1.6

- Secure Messaging update
- Audit improvements
- MIS improvements
- Rework of portal authentication service
- Agent assignment enhancements
- R&E web service extensions
- Integration tier
- Click to add
- R&E enhancements
- ISV test service enhancements
- Digsig enhancements
Appendix D – Useful Links

The UK Government Gateway:  www.gateway.gov.uk
Office of the e-Envoy:  www.e-envoy.gov.uk
GovTalk:  www.govtalk.gov.uk
Developer site:  www.govtalk.gov.uk/gateway_partnerlink
W3C:  www.w3c.org
IETF:  www.ietf.org
Appendix E – Contacts

Please check the details and the developer link in Appendix B (developer information) which contain a great deal of more in-depth information.

Departments requiring assistance in developing or launching Gateway-enabled services should send an email request to:

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

Queries from partners or developers, and comments about the site structure or content, of the Gateway Partnerlink site should be sent to:

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