Government Gateway

Portal Infrastructure

Statement of Service Requirement
Government Gateway
Service Specification

Contents

CONTENTS 2

1 INTRODUCTION 5
1.1 Aim of this document 5
1.2 Scope of this document 5

2 BACKGROUND 6
2.1 Modernising Government 6
2.2 Government Portal 6
2.3 What is the Government Gateway? 8
2.4 Success Factors 9
  2.4.1 Value added and service take-up 9
  2.4.2 Performance 9
  2.4.3 Management information 10

3 GATEWAY FUNCTIONAL REQUIREMENTS 11
3.1 Transaction management requirements 11
3.2 Authentication requirements 12
3.3 Security requirements 14

4 ARCHITECTURE REQUIREMENTS 16

5 INTERFACES TO DELIVERY CHANNELS 18

6 INTERFACES TO DEPARTMENTS 20

7 CLIENT SERVICES SUPPORT 22

8 SUPPORTING TOOLS AND TECHNIQUES 23

9 PROJECT MANAGEMENT REQUIREMENTS 24
9.1 Initial Required Information from Contractors 24
9.2 Human Resources 24
9.3 Quality management 25
9.4 Project management 25
9.5 Configuration Management 26
9.6 Service management requirements 26
9.7 Management information requirements 27
9.8 Legislation 28
9.9 Gateway Future Development 28

10 CAPABILITY 29
1 Introduction

1.1 Aim of this document

Central IT Unit is seeking to award a contract for the development and provision of the Government Gateway. The aim of this document is to define the requirements for this service. This document is a Statement of Service Requirement (SSR) and is considered a constituent part of the Invitation to Tender documentation for the Government Gateway Service.

1.2 Scope of this document

This document covers the Government Gateway procurement. Background details of the wider Government Portal and in particular the “me.gov” and Data Interoperability Framework component are provided for context, but are outside the scope of this procurement.

This document covers all aspects of the requirement for Government Gateway service provision, including functional and operational characteristics and development requirements.
2 Background

2.1 Modernising Government


A key commitment of the White Paper is Information Age Government. Government has begun to harness new technology to meet the needs of citizens and businesses, as well as to modernise itself.

Key benefits of Information Age Government will be better service delivery and more efficient working. The development of electronic service delivery is integral to the Government’s aim to deliver improved public services. This requires “joined up” working between different parts of Government, and providing convenient ways for the citizen and businesses to communicate with Government and receive services.

The Government Portal will facilitate joined up Government and electronic service delivery.

2.2 Government Portal

A Government Portal feasibility study has been conducted by PA Consulting (http://www.citu.gov.uk/portals/portalmenu.htm). The Government Portal will consist of two key components:

1. The Government Gateway will link the widest possible range of government services and information. It will provide a standardised interface through which a multiplicity of delivery channels can provide services, connected to a multiplicity of back office processes throughout Government and beyond. It will also provide value-added services such as transaction management, data standardisation and third party authentication for the citizen to Government departments.

2. me.gov will operate as a “front end” to the Government Gateway. It will enable the citizen to access Government services and information electronically and to develop a personal profile with respect to their dealings with Government. It will facilitate the organisation of public services around the needs of the citizen and will promote seamless service delivery. It will also realise the concept of joined up Government by enabling the citizen to notify different parts of Government of name and address simply and electronically in one transaction.

me.gov will ultimately be only one of a wide range of services available through the Gateway. Other services may be provided directly by Departments or through intermediaries such as Local Authorities, the Post Office and the private sector.
In addition, as well as interaction with Departments through the Government Gateway, me.gov will be required to work directly to existing and developing departmental systems, portals and services prior to their connection to the Government Gateway.

Figure 1 (below) illustrates the Portal structure and positioning within which the Government Gateway will operate.

![Figure 1: Structure and positioning of Government Portal](image)

The Gateway is being procured separately from me.gov for several reasons.

- Gateway, as a major piece of HMG infrastructure, requires a different development skill set than the customer facing internet based me.gov.
- The management and control of the service will have different requirements to that of me.gov.
- The eventual ownership of the two procurements may differ.
- Gateway must support multiple services and multiple front-ends, not just me.gov
- The presentation layer needs to be supervised and focused on the citizen whilst the Gateway is focused on providing an industrial strength architecture for security, authentication and transaction services.
2.3 What is the Government Gateway?

The Gateway is the centrepiece of "joined up" Government, and it is expected that all services that are to be "joined up" in this manner will use the Gateway to facilitate the needed cross Governmental interaction.

The gateway will act as an intelligent hub, providing a common access point for a number of service & delivery channels to a number of back office governmental services, and a transaction engine, with application functionality to provide services such as audit, authentication and security.

As such, the Gateway provider will be required to implement diverse service details in conjunction with the me.gov and / or other front-end service providers. Interdepartmental business logic will exist in the Gateway where this is necessary and not appropriate within departmental processes.

The Gateway will be required to provide data and service interfaces between multiple service delivery channels and multiple back office processes across Government and beyond.

Delivery channels will include the "me.gov" service, and other services that may be provided directly by Departments or through intermediaries such as Local Authorities, the Post Office and the private sector.

Back office processes and systems will be connected to the Gateway in order to exchange and/or process information and/or elements of services to the delivery channels. These processes may include (but may not be restricted to) those of Central Government Departments, Local Authorities, Non-Departmental Public Bodies, the NHS and the Police. They may also include value-added services from the private sector.

It should be noted that some organisations, such as local authorities, may act as both service providers, delivery channels and back office agents, and may be required to connect to the Gateway in two places.

Based on the above, it is envisaged that the Government Gateway will be a piece of "industrial strength" infrastructure. This infrastructure will provide the means by which end-to-end customer services (e.g. Change of Address notifications and tax returns) will be overlaid.

The Product Management Group is a group consisting of key service owners and product managers e.g. for change of address or tax return filing. The Product Management Group is responsible for translating these specific end-to-end services into detailed requirements for the delivery channels (including me.gov) and the Gateway. These requirements must be met by each of the functions within the portal as a whole in order for the service to work effectively. There will therefore be a contractual requirement to work with delivery channel providers and back office process managers in order to implement the emerging end-to-end services.

The Gateway will be run as a managed service.

The Contractor should:
Requirement 1 - demonstrate an understanding of the role of the Gateway within the overall vision for joined up Government

2.4 Success Factors

The success factors for the Gateway projects fall into three areas; value added and service take-up, performance and management information. Each of these is discussed below.

2.4.1 Value added and service take-up

The take-up of the Gateway will depend upon the value that it adds to services which are provided through it. The added value is derived from FUNCTIONALITY (transaction management, interdepartmental business logic, service routing, elements of service management, authentication, data standardisation) and ECONOMY OF SCALE SAVINGS through providing such functionality centrally.

Take-up success can be measured exponentially, derived from the rate of which different types of services are connected. The rate of back office connection and rate of authentication service connection will also be important.

The extent to which the authentication market grows toward critical mass and is accepted is also a success metric.

<table>
<thead>
<tr>
<th>Success Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximise economy of scale savings</td>
</tr>
<tr>
<td>Maximise the number of connected channels</td>
</tr>
<tr>
<td>Maximise the number of connected departments</td>
</tr>
<tr>
<td>Maximise the number of connected authentication partners</td>
</tr>
<tr>
<td>Successful integration with me.gov and back offices</td>
</tr>
</tbody>
</table>

2.4.2 Performance

The success of the Gateway will be critically dependent upon its performance in facilitating services. Metrics will include availability, resilience and Gateway-dependent service delays.

Success-enhancing performance features will include transaction status visibility and high functionality.

<table>
<thead>
<tr>
<th>Success Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>High availability</td>
</tr>
<tr>
<td>High resilience</td>
</tr>
<tr>
<td>Minimal service delays</td>
</tr>
<tr>
<td>Maximise number of successful transactions</td>
</tr>
</tbody>
</table>
Demonstrably secure operation over the period
High number of successful authentication requests

2.4.3 Management information

Feedback information on the operational success of the Gateway will be available by means of the service managers of those systems and services connected to the Gateway. Management information will only be requested where it is a requirement for Government action and is likely to consist of such information as number of transactions, types of transaction and the department that deals with the transaction.

However, the success of the Gateway will be critically dependent upon feedback from service providers, departments, authentication service providers and other connected parties. A mechanism will be required to allow feedback from parties other than the contractor to be formalised, measured and acted upon.

<table>
<thead>
<tr>
<th>Success Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive Feedback</td>
</tr>
<tr>
<td>Accurate Information</td>
</tr>
<tr>
<td>Quality of Information</td>
</tr>
<tr>
<td>Speed of response</td>
</tr>
</tbody>
</table>

The Contractor should:

Requirement 2 - propose a feedback / monitoring mechanism and describe how this will be used to improve service

Requirement 3 - contractors are invited to provide their own additional Successful Factors if this is felt appropriate.
3 Gateway functional requirements

3.1 Transaction management requirements

The Gateway will be required to provide complex transaction management for a wide range of yet undefined end-to-end services. This transaction management will involve managing requests for information from one or more sources providing co-ordination between multiple connected systems.

Transaction management requirements will include, but not be limited to:

- Service-specific business logic allowing the incoming data from the front-end delivery channels to be split and sent to the various departments and also allowing data from back office processes to be integrated and passed to the user as applicable to the specific services delivery channel.

- Aggregation and disaggregation of transactional data will also be required between Government departments.

- Financial transaction processing, auditing and receipting;

- Auditing for data protection and other purposes (the Contractor should note that requirement to comply with the Data Protection Act via the principle of informed consent);

- Data Transformation and Routing

- Transactional integrity

- Authentication service processing.

The Gateway will be required to manage information flow as well as services. Contractors will be required to provide sophisticated content sourcing and distribution to and from a variety of points within and beyond the public sector. Content sources may include simple web information or complex database search results. Content must be presented to me.gov and other delivery channels in a consistent and defined manner (see Requirements in Chapter 5).

The Gateway will be required to manage financial transactions, possibly including debit or credit card payments. Financial transaction management will need to observe all relevant principles of propriety and legislation. Liability and fraud prevention issues must be addressed.

The Contractor should:

Requirement 4 – describe a detailed proposal for the transaction management functionality architecture to be employed;

Requirement 5 – explain how the transaction management architecture will scale to incorporate multiple services (as yet undefined) as they emerge, which could consist of one or many transactions ;
Requirement 6 – provide a proposal for a co-operative working regime to achieve service functionality within the Gateway (including “me.gov” services);

Requirement 7 – provide proposals for the engagement of Government in comprehensive functionality and design reviews.

Requirement 8 - describe the concept, process and architecture for the management of information content throughout the Gateway

Requirement 9 - describe proposals for the management of financial transactions through the gateway. Address liability issues.

3.2 Authentication requirements

The gateway must provide interfaces to a range of third-party authentication services in order to allow citizens and businesses to identify themselves to Government. These services will include, but not be limited to, digital certification services and user ID/password services.

The Government will develop and maintain a list of approved authentication service providers, based on published criteria and allocate each transaction to one of three authentication trust levels, from level 1 (lowest) to level 3 (highest), or state that there is no requirement for authentication (level 0).

The definitions of these levels are provided in the Authentication Framework (see http://www.iagchampions.gov.uk/guidelines/authentication/)

Government is currently working with tScheme Ltd, the UK’s co-regulatory regime for providers of encryption services, to agree a number of profiles which set out the requirements for authentication services meeting each trust level. Entry to the list of approved authentication service providers will be dependent upon conformance to the requirements of a Government approved profile (whether or not the supplier is a member of tScheme).

The interface between the Gateway and authentication services must provide interoperability with any such Government-approved authentication service. It must also be scalable to support the requirements of continuously emerging services. Like the delivery channel and back office interfaces, it must be based upon published standards in accordance with the requirements of the Government Interoperability Framework. A draft version of this Framework is included in Appendix D of this document. It is provided as a snapshot of the current thinking and is subject to change.

The authentication interface will require secure connectivity: contractors are required to outline how such connectivity will be offered to authentication service providers.

The selected service provider will be required to work co-operatively with a wide range of 3rd party authentication service providers across the public and private sectors, in addition to any value-added ancillary service providers which may be required (such as specialist time-stamping services for example). In particular, the selected service provider will be required to co-operate with tScheme in adopting common standards and procedures for connection of authentication service providers.
It is envisaged that 3rd party authorisation service providers will supply digital certificate services. However, there is also a requirement to integrate a user ID / password based authentication solution. Contractors will be required to integrate the current Inland Revenue owned authentication service (currently operated by EDS IRD). This service will be considered an essential integral component of the Gateway.

With the exception of this user ID / password authentication requirement it should be stressed that authentication services themselves are not integral to the Gateway, and any Contractors proposing to provide authentication services in addition to core Gateway functionality (as specified herein), should do so outside the scope of this procurement.

Contractors will be required to ensure that authentication services accessible from the Gateway and available for use via me.gov are available to all channels that require it.

In addition to user authentication, the Gateway will be required to authenticate itself to delivery channels (and vice versa). It will also be required to authenticate itself to back office processes and authorisation service providers.

The Contractor should:

**Requirement 10** – describe how the Gateway will scale to support an undefined number of authentication service providers

**Requirement 11** – describe how the Gateway interface to authentication services will observe the published standards of the Government Interoperability Framework

**Requirement 12** – provide a proposal for a co-operative working regime to achieve efficient connection of authentication services to the Gateway. In particular detail plans for close co-operation with tScheme.

**Requirement 13** – describe how secure network connectivity between the Gateway and diverse authentication services will be achieved. Outline plans for the use of the GSI community, and detail any requirements for the use of networks other than the GSI community.

**Requirement 14** – describe a proposal for the incorporation of third-party authentication services into the initial service offering.

**Requirement 15** - describe how the Gateway will interface to various authentication service providers

**Requirement 16** - describe how the Gateway will incorporate the current Inland Revenue owned user ID / password authentication system.

**Requirement 17** - describe how the Gateway will authenticate itself to me.gov and other delivery channels, back office processes and authentication service providers.

**Requirement 18** - describe how authentication services accessible though me.gov will be available to other channels.
3.3 Security requirements

The Gateway will have a "clean" element connected to GSI and a "dirty" element, connected to untrusted networks, including the Internet. A security architecture will be required which facilitates this separation in accordance with HMG policy.

There will also be a need to protect the confidentiality and integrity of information held on or passing through the gateway, and to protect the gateway and systems connected to it from accidental or deliberate denial of service attacks.

The Gateway must meet in full the requirements of the IAG security framework. This framework includes a high level requirements document and detailed guidance on business services (currently only web security but more to be added as demand grows), trust services (read in conjunction with the authentication framework) and confidentiality services. (NB detailed guidance is currently only available in draft form and is subject to consultation and change). There will be an eventual requirement to comply with all guidance – however, in the event of changes, reasonable transition periods may be negotiated with Government.

The 'clean' side of the gateway will be considered as a RESTRICTED system with a high integrity and availability requirement, and must conform to the requirements of the Manual of Protective Security pertaining to such systems. The vendor will also be required to meet the requirements of the Data Protection Act.

The Contractor should:

Requirement 19 - describe how they will meet the requirements of the IAG security framework;

Requirement 20 - describe how they will meet the requirements of the Manual of Protective Security

Requirement 21 - provide an analysis of the risks and vulnerabilities to which the Gateway will be subject, and the countermeasures proposed.

Requirement 22 - describe the approach to separating 'clean' and 'dirty' sides of the gateway.

Requirement 23 - explain the approach to providing security assurance in the design and build phases.

Requirement 24 - explain the approach to security audit and IT healthchecks, monitoring for security incidents and responding to them and security accounting and audit

Requirement 25 - explain the physical security measures applicable to the proposed site for the gateway

Requirement 26 - explain the personnel security approach which it will adopt

Requirement 27 - explain how they will obtain and maintain BS7799 accreditation for the system under the c:cure scheme.
Requirement 28 - detail the experience of developing similar systems providing transactional interfaces between the Internet and secure back-office processes.

Requirement 29 – propose a comprehensive Disaster Recovery plan.

Requirement 30 - provide detailed GSI accreditation plans.
4 Architecture Requirements

In order to support the above functionality, the Gateway requires a scalable architecture.

Transaction rates are difficult to quantify, although the PA Consulting feasibility study (http://www.citu.gov.uk/portals/portalmenu.htm) contains some estimates. Contractors will be required to describe in some detail the scalable network architecture that will achieve this.

Connections will be required to a multiplicity of delivery channels and services, back office processes and third party services (e.g. authentication). Contractors will be required to estimate, monitor and manage the capacity of the infrastructure to handle the resultant traffic. The contractor should note that constituent transactions may be single or multiple, and may be batched or interactive, when calculating this capacity.

Availability and resilience will be two critical requirements of the architecture. Any failure here will lead to an effective denial of service for the full range of Government service provision. The Gateway will form part of the Critical National Infrastructure.

The Critical National Infrastructure consists of systems in the public and private sectors that are so important to national life that a successful large-scale disabling attack on them, leading to major loss of service, would have serious economic or social consequences and would be of immediate concern to the Government.

The data standards should conform to the Government Interoperability Framework, available in Appendix D of this document in a draft form. In particular it will adhere to the overall XML strategy for data integration whilst conforming to the Internet and World Wide Web stack of standards for interconnectivity.

Preference will be given to solutions that use open standards and market leading products.

The Contractor should:

Requirement 31 – detail the overall architecture of the Gateway and the middleware to be employed.

Requirement 32 - describe the development approach for constructing the middleware

Requirement 33 – provide an architecture diagram

Requirement 34 - describe proposals to ensure scalability and resilience including that of connections to multiple networks, along with plans for how the resilience and availability of the system will be maintained as it is scaled up and scaled down. Responsiveness should be defined and the extent of any redundancy should be demonstrated.

Requirement 35 - provide an architecture diagram describing what will be contained within the Gateway, as well as the interfaces and information flows from delivery channels, back office processes and authentication service providers.
Requirement 36 - specify the operating system and development standards / tools / languages which will be used in the Gateway

Requirement 37 - describe how end-to-end services will be translated into technical implementations

Requirement 38 - describe proposals for the use of open or public standard Application Programming Interfaces (APIs), and also any proposals to allow third parties to configure the infrastructure to deliver end-to-end services

Requirement 39 – provide estimates of the initial minimum bandwidth and how it will be scaled up

Requirement 40 – provide a proposal for continuous liaison with the “me.gov” Contractor in order to minimise scaling mismatch on this key interface.

Requirement 41 - describe the intended regime for responding to multiple delivery channel providers for requests to develop the Gateway element of end-to-end services

Requirement 42 - provide, and describe, a diagram describing all interfaces to external parties

Requirement 43 – provide an infrastructure growth plan, including capacity management procedures, and liaison with third parties where capacity would be affected. This should include mechanisms for coping with a mismatch of traffic demand and network capacity, both at service launch and thereafter.

Requirement 44 – propose target availability rates for the Gateway, and how these will be measured and maintained. (Contractors are invited to provide real availability figures from reference sites should they consider this useful).

Note that in responding to the architecture requirements in this section, the Contractor should explicitly respond in terms of the development, test and operational phases of the project.
5 Interfaces to Delivery Channels

Delivery channels will include the “me.gov” service and other services that may be provided directly by Departments or through intermediaries such as Local Authorities, the Post Office and the private sector. Furthermore, delivery channels may make use of a variety of access media, including Internet-enabled PCs, kiosk access, digital television, call centres and 3G mobile telephony.

The interface between the Gateway and these delivery channels must be capable of supporting a wide and as yet undefined range of services. It must be scalable to support the requirements of as yet unknown service quantities. It must also be based upon published standards in accordance with the requirements of the Government Interoperability Framework. A draft version, number 0.3, of this Framework is included in Appendix D of this document. It is provided as a snapshot of the current thinking and is subject to change.

Furthermore, the services connected will involve access via a number of different access media, including the internet, kiosks, digital television, and 3G mobile telephony. The Contractor should ensure that nothing in the Gateway restricts the choice of access media that is available to delivery channels.

The interface between the Gateway and these delivery channels will require network connectivity, which must be provided by means of the Internet, the Government Secure Intranet (GSI), or an other appropriate network. Network connectivity may differ by service. Contractors are required to describe how such connectivity will be provided, and the rationale for choice of network.

The Product Management Group is a group consisting of key service owners and product managers e.g. for change of address or tax return filing. The Product Management Group is responsible for translating these specific end-to-end services into detailed requirements for the delivery channels (including me.gov) and the Gateway. These requirements must be met by each of the functions within the portal as a whole in order for the service to work effectively.

The selected Contractor will be required to work co-operatively with the “me.gov” Contractor, other emerging delivery channel service providers as they emerge, CITU and their appointed representatives and consultants and the Product Management Group in order to agree the implementation of the interface standards. There will also be a requirement to work co-operatively in connecting service providers as they emerge. This activity is an important element of the programme and contractors will be required to explain how they will resource it.

The Contractor should:

**Requirement 45** – detail technical proposals for connection of the Gateway to delivery channels (including me.gov), and the resource implications of this.

**Requirement 46** – describe how the Gateway architecture will scale to interface to an undefined number of service partners. The contractor should note that transactions may include both synchronous and asynchronous operation across any interface.
Requirement 47 – describe how the Gateway will interface with service providers and delivery channels will observe the published standards of the Government Interoperability Framework. A draft version, number 0.3, of this Framework is included in Appendix D of this document. It is provided as a snapshot of the current thinking and is subject to change.

Requirement 48 – provide a proposal for a co-operative working regime with the partners identified above in order to agree implementation standards. This is to include testing and proving capability which will reflect the eventual live operation.

Requirement 49 – provide a proposal for a co-operative working regime to achieve efficient connection of service providers to the Gateway.

Requirement 50 – demonstrate that the Gateway will impose no limitations on the access media options for connected services.

Requirement 51 - explain how a channel provider, using a network connection from a major provider of data connection services, will connect to the Gateway

Requirement 52 - provide a proposal for working with other connecting service providers.
6 Interfaces to Departments

Back office processes will be connected to the Gateway in order to exchange and/or process information and/or elements of services to the delivery channels. These systems may include (but not be restricted to) those of Central Government Departments, Non-Departmental Public Bodies, the NHS and the Police. They may also include value-added services from the private sector. The contractor is advised to view Appendix B of this document for specific mandatory HMCE and IR requirements.

The interface between the Gateway and these processes must be capable of exchanging data across the full (as yet undefined) range of Government services, and across the full range of back office data types. It must also be scalable to support the requirements of any emerging connections. Like the service interfaces, it must be based upon published standards in accordance with the requirements of the Government Interoperability Framework. A draft version, number 0.3, of this Framework is included in Appendix D of this document. It is provided as a snapshot of the current thinking and is subject to change.

This interface will require secured connectivity, which will include connection to the GSI and may include connection to other secure networks at the RESTRICTED or lower levels. However, it is acknowledged that network connectivity may differ for different back office processes. Contractors are required to describe how such connectivity will be provided.

Contractors are required to present plans for achieving accreditation of the Gateway to connect to the GSI. Contractors are expected to understand the GSI accreditation process. It is assumed that the Gateway will connect as a unique entity. Contractors are therefore advised that they will not be in a position to "piggy back" on to an existing Departmental GSI connection, nor on any wider connection to a GSI extranet or subnet. It is assumed that the Gateway will have a dedicated connection to the GSI (see Chapter 2 - Security).

The Product Management Group is a group consisting of key service owners and product managers e.g. for change of address or tax return filing. The Product Management Group is responsible for translating these specific end-to-end services into detailed requirements for the delivery channels (including me.gov) and the Gateway. These requirements must be met by each of the functions within the portal as a whole in order for the service to work effectively.

The selected Contractor will be required to work co-operatively with a wide range of back office process managers across the public sector and the Product Management Group, in addition to value-added content providers from the public or private sectors. The extent of such co-operation will be largely driven by the service providers and delivery channels which utilise the services of the Gateway.

In addition, the Contractor is expected to perform an internal marketing role within government to facilitate the take-up of services. This could involve such items as "coffee-table" documents, call handling, facilitated workshops or technical labs. Contractors are encouraged to provide further proposals in this area.

The Contractor should:
Requirement 53 - detail technical proposals for connection of the Gateway to back office processes and the resource implications of this.

Requirement 54 – describe how the Gateway will scale to support an undefined number of back office processes. The contractor should note that transactions may be synchronous or asynchronous.

Requirement 55 – describe how the Gateway interfaces with back office processes will observe the published standards of the Government Interoperability Framework. A draft version, number 0.3, of this Framework is included in Appendix D of this document. It is provided as a snapshot of the current thinking and is subject to change.

Requirement 56 – provide a proposal for a co-operative working regime to achieve efficient connection of back office processes to the Gateway.

Requirement 57 - provide a proposal for a co-operative working regime with the Product Management Group.

Requirement 58 - provide and describe a diagram showing all interfaces to external parties

Requirement 59 – describe how secure connectivity between the Gateway and diverse back office processes will be achieved. Describe plans for the use of GSI, estimate the bandwidth required for this connection and detail any requirements for the use of networks other than GSI.

Requirement 60 - provide a description of how the Contractor proposes to achieve take-up of services within the departments, and how this will be resourced.

The Contractor should note the relevance of the "Infrastructure Growth" requirement in Chapter 4 as a reference to the above requirements.

The contractor should note that in responding to the architecture requirements in this section, they should explicitly respond in terms of the development, test and operational phases of the project.
7 Client Services Support

Many stakeholders will depend upon continuous operation of the Gateway for their business continuity. This includes Government Departments, delivery channels/service providers and authentication service providers.

Each stakeholder will require the provision of timely support in the event of incorrect operation, and in the event of service/system queries. As the Gateway does not directly serve citizens and businesses, this support will need to be targeted at service providers and process managers rather than the general public. Consequently, the market to serve will be small, but the quality, depth and expertise levels must be high.

It is recognised that the Gateway will form one element of many end-to-end services, but that the selected Contractor will be responsible for supporting only the Gateway element of any service. The selected Contractor will be expected to identify in a timely fashion whether any reported incorrect operation or query relates to the Gateway, prior to providing support. The selected Contractor will be penalised for failing to respond to problems for which he/she is responsible.

The Contractor should:

**Requirement 61** - describe proposals for providing adequate support to all stakeholders.
8 Supporting Tools and Techniques

Translation of end-to-end service requirements into Gateway configuration will necessitate the development and provision, by the Contractor, of "service creation tools" using the Gateway architecture. Such translation will occur on a rolling basis. The Contractor should be aware of the links with the API requirements in Chapter 4 - Architecture Requirements.

Tools will also be required to facilitate systems testing, operational fault detection and fault repair.

The Contractor should:

**Requirement 62** - describe proposals for the provision of service creation tools

**Requirement 63** - describe proposals for the provision of test and fault management tools.

**Requirement 64** - describe proposals for the provision of configuration management tools

**Requirement 65** - propose the life cycle model to be adopted for the provision of new services and the tools that will be used

**Requirement 66** - describe how stress and regression tools will be developed, deployed and used

**Requirement 67** - describe any tools that will be used for service creation via API's
9  Project Management Requirements

9.1  Initial Required Information from Contractors

Certain information is required about the project from the Contractor. This includes the primary and secondary contracts for the company responses, and a plan to ensure the procurement timetable can be met.

The Contractor should:

Requirement 68 – identify and provide primary and secondary contact details for the individuals with responsibility for the Contractor’s response during the procurement phase of the Gateway project.

Requirement 69 – identify and provide contact details for the senior manager with overall responsibility for the Contractor’s performance during the procurement phase of the Gateway project.

Requirement 70 – describe a plan as to how the procurement timetable will be met.

9.2  Human Resources

The Gateway project will be challenging in scope, complexity and timescale. It may involve the management of complex requirement changes and will certainly be affected by fast-changing external factors, such as amount and type of competition and number of registered users and services. It will need exceptionally strong project management. As such, we are looking for a team to be proposed by the Contractor to demonstrate that the Contractor recognises these challenges. The make-up of this team will be a key factor during evaluation. It is expected that the contractor will build confidence by ensuring that the team is ideal for the purpose.

The selected Contractor will be expected to work closely with CITU on the development and service provision of the Gateway. Particular emphasis will be placed upon flexibility and responsiveness.

The Contractor should:

Requirement 71 – identify and provide contact details for the appointed project manager with overall responsibility for the Gateway project.

Requirement 72 - provide details of the proposed project team, including the skills and experience of the individuals.

Requirement 73 – estimate, with justification, the resource commitment considered necessary from Government during the development and operational phases of the project.

Requirement 74 – describe how a close working relationship between CITU, the Contractor and participating third parties can be established and maintained.
Requirement 75 – define the escalation procedure to be followed in the event that issues are not dealt with to the satisfaction of Government.

9.3 Quality management

The size and complexity of the Gateway project will necessitate the rigorous application of quality standards. Contractors should illustrate their commitment to quality by outlining the specific quality measures to be applied to this project.

The Contractor should:

Requirement 76 – provide details of ISO9001 accreditation, including accreditation scope.

Requirement 77 - produce a quality plan for the project

Requirement 78 – illustrate how quality standards will be applied to the development and service provision of the Gateway.

9.4 Project management

The success of the Gateway project will require project management of the highest standard. Management processes must be appropriate to the project type and must provide a high degree of visibility and responsiveness to the Portal Project Board.

A project plan will be required from the Contractor as a key element of responses. This plan must cover the development phase of the project, including test activities, and must include all aspects of project management, including but not limited to:

- Project definition and scoping
- Work breakdown structure
- Risk breakdown structure
- Risk management process
- Assumptions
- Constraints to the project
- Acceptance Criteria
- Deliverables definition
- Project schedule
- Subcontracting plan
- Quality plan
- Resource plan
- Cost breakdown
- Identification of items to be supplied by Government or agents of Government
- Materials purchase plan and schedule
- Integration plan, test plan

The Contractor must be prepared to make these documents available across Government.
The first deliverable during the project development phase will be a Project Initiation Document (PID), created by the Contractor in conjunction with CITU. All further funding will be dependent upon agreement of the PID with CITU.

The Contractor should:

**Requirement 79** – provide a project plan, including Gantt chart, covering the development phase of the Gateway project.

**Requirement 80** – identify key project risks and provide a risk management plan, covering both content and process.

**Requirement 81** – provide a critical path analysis for the project plan.

### 9.5 Configuration Management

Configuration management is the management of products, facilities and processes, focusing on their requirements including changes and assuring conformance to best practice in each case.

A best practice configuration management process includes accommodation of change, ensuring the setting and reuse of standards and best practices, assuring that all requirements remain clear concise and valid, communicating all those points above to all parties involved and finally assuring performance in each case.

The Contractor should:

**Requirement 82** - detail how configuration management will be used within the Gateway project, including such items as document management, change control / version management and quality control.

**Requirement 83** – propose a complete documentation set to be provided over the course of the contract.

**Requirement 84** – describe the proposed document management regime.

### 9.6 Service management requirements

Project success will also require excellent service management skills. Management processes must be appropriate to the project type, must be adequate for the complexity and scale of the systems employed, and must be responsive enough to support fast-moving Internet service delivery. A very high degree of visibility to the Portal Programme Board and management groups will be mandatory.

A service management plan will be required from the Contractor as a key element of responses. This plan must cover the operational phase of the project, and must include all aspects of service management, including but not limited to:

- Service definition and scoping
- Draft Service Level Agreements (SLAs) concerning availability, number of connections, reliability and other relevant measures for delivery channels (including me.gov)
• Identification of key risks
• Risk management process
• Change management process
• Operational process definition
• Role and responsibilities
• Subcontracting plan
• Quality plan
• Resource plan
• Exit plan
• Cost breakdown
• Identification of items to be supplied by Government or Government agents
• Service launch plan
• Performance measurement regime
• Reporting to the Portal Programme Board.

Particular emphasis should be given to external interface management. Emphasis should also be given to the multi-way feedback processes that are necessary for continuous service improvement.

A programme for responding to incremental connection of Government Departments, third party services (e.g. authentication) and delivery channels/services to the Gateway over the life of the SPA must supplement the service management plan.

The Contractor should:

**Requirement 85** – provide a service management plan covering the development phase of the Gateway project.

**Requirement 86** – identify key operational risks and provide a risk management plan, covering both content and process.

**Requirement 87** – describe a programme for responding to connection requests from Government departments to the Gateway.

**Requirement 88** - describe a programme for responding to connection requests from service providers.

**Requirement 89** - describe a method of ensuring the Portal Project Board have high visibility of the work conducted.

**Requirement 90** - describe how the contractor will act as an implementing / marketing entity in order to facilitate take-up from back offices

### 9.7 Management information requirements

The first requirement for management information addresses the need to run a service that is trusted by the citizen, Government and the law. Information must be available to provide a full audit trail of Gateway actions that will withstand legal scrutiny.

The second requirement for management information addresses the need to achieve the critical success factor of positive feedback by all connected parties.
The achievement of success requires management information to be used as part of an effective communication strategy to all connected parties including service providers, authentication service providers and back office process managers.

The Contractor should:

**Requirement 91** – propose a regime for the capture, processing, storage, distribution and action taken as a result of management information.

**Requirement 92** – define the management information to be provided and explain how these measures will prove that the CSF’s are being satisfied.

**Requirement 93** – define a management-targeted communication strategy employing management information.

**Requirement 94** - describe your understanding of legal requirements of types of management information that must be supplied.

### 9.8 Legislation

The Contractor is obliged to conform to the following legislation in constructing the Gateway:

- Data Protection Act 1998
- Police and Criminal Evidence Act 1984
- Computer Misuse Act 1990
- Disability Discrimination Act 1995

The Contractor should:

**Requirement 95** - provide a statement on how the legislation will be complied with.

### 9.9 Gateway Future Development

The Contractor should:

**Requirement 96** – provide development strategy for the Gateway.

**Requirement 97** – provide service provision strategy for the Gateway.

**Requirement 98** – provide funding proposal for Gateway.

**Requirement 99** - provide a list of issues that the contractor feels has not been covered in this document concerning the portal as an entity.
10 Capability

As far as is known, the scale and complexity of the Government Portal project is greater than any similar project attempted before in Government. However, the requirement for scalable network connectivity supporting published data standards, transaction management and authentication is not new.

Contractors with existing experience in this field are invited to detail this in their proposals, as a review of previous experience will form a significant element of the evaluation. Contractors are advised to include specific details of the relevance of each of the examples their proposal. For each example, the Contractor should identify the period over which the project was undertaken and the aspect of the project for which responsibility is claimed.

The Contractor should:

Requirement 100 - provide details of experience in meeting similar requirements.

Requirement 101 - provide details of relevant reference sites, and contact names at these sites
APPENDIX A: Definitions

"CoA" shall mean Change of Address

"Development" means all activities from concept, design, build etc to initial operation but does not include operational activity thereafter.

“Gateway” and “Government Gateway” shall be considered interchangeable.

“GTC” means Government Telecomms Contracts

“GTC Contractors” shall mean those Contractors invited under the GTC Framework Agreement to participate in this procurement

"GSI" shall mean the Government Secure Intranet

“Invitation to Tender (ITT)” shall mean the documentation issued to selected Contractors to participate in the Government Gateway procurement.

“Portal” or “Government Portal” shall mean the aggregation of the Gateway and the ‘ME.Gov Service’ and the Data Interoperability Framework, or the aggregation of the Gateway and other channels.

“Selected Contractor” shall mean the successful Government Gateway bidder.

“Service Provision Agreement (SPA)” shall mean the SPA of the GTC Framework Agreement.

“SSR” shall mean the Statement of Service Requirement issued with the Invitation to Tender.