Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications

NATIONAL PROFILE UK

April 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Richard Trevorah, xidm Limited

Company's name: Siemens - Lawfort

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°1

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6485/5938

Executive summary

The objective of the project is to analyse the requirements in terms of interoperability of electronic signatures for different eGovernment applications and services taking into account the relevant provisions of Directive 1999/93/EC on a Community framework for electronic signatures and their national implementation as well as the report on the Directive and the standardisation activities on the interoperability of electronic signatures.

This document represents the current situation regarding the use of eSignatures in UK eGovernment applications.

Table of Contents

EXECUTIVE SUMMARY 3

1 DOCUMENTS 6

1.1 APPLICABLE DOCUMENTS 6

1.2 REFERENCE DOCUMENTS 6

2 GLOSSARY 8

2.1 DEFINITIONS 8

2.2 ACRONYMS 9

3 INTRODUCTION 10

3.1 EGOVERNMENT STRUCTURE 10

4 EGOVERNMENT AND ESIGNATURE REGULATIONS 12

4.1 ESIGNATURES REGULATORY FRAMEWORK 12

4.2 EGOVERNMENT REGULATORY FRAMEWORK 12

5 EGOVERNMENT APPLICATIONS USING ELECTRONIC SIGNATURES 14

5.1 GOVERNMENT GATEWAY 14

5.1.1 APPLICATION IDENTIFICATION 14

5.1.2 ESIGNATURE DETAILS 14

5.1.2.1 Legal Aspects 14

5.1.2.2 Technical Aspects 14

5.1.2.3 Organisational Aspects 15

5.1.3 INTEROPERABILITY 16

5.1.4 MISCELLANEOUS 16

5.1.5 ASSESSMENT 17

5.2 E-CONVEYANCING 17

5.2.1 APPLICATION IDENTIFICATION 17

5.2.2 ESIGNATURE DETAILS 17

5.2.2.1 Legal Aspects 17

5.2.2.2 Technical Aspects 17

5.2.2.3 Organisational Aspects 19

5.2.3 MISCELLANEOUS 19

5.2.4 ASSESSMENT 19

5.3 OIL & GAS TRUST SCHEME 19

5.3.1 APPLICATION IDENTIFICATION 19

5.3.2 ESIGNATURE DETAILS 20

5.3.2.1 Legal Aspects 20
5.3.2.2 Technical Aspects 20
5.3.2.3 Organisational Aspects 22
5.3.3 INTEROPERABILITY 22
5.3.4 MISCELLANEOUS 22
5.3.5 ASSESSMENT 22

6 GENERAL ASSESSMENT 23

7 OPERATIONAL AND PLANNED APPLICATIONS 24

7.1 APPLICATIONS AT THE NATIONAL LEVEL 24

8 ANNEX A: CONTACT DETAILS OF NATIONAL CORRESPONDENTS 25

8.1 PRIMARY CONTACT 25

8.2 ALTERNATIVE CONTACT 25

9 ANNEX B: NATIONAL REGULATIONS DETAILS 26

10 ANNEX C: APPLICATION QUESTIONNAIRES 27

10.1 GOVERNMENT GATEWAY 27
10.1.1 APPLICATION IDENTIFICATION 27
10.1.2 ESIGNATURE DETAILS 29
10.1.3 INTEROPERABILITY 31
10.1.4 MISCELLANEOUS 32
10.1.5 ASSESSMENT 32

10.2 E-CONVEYANCING 33
10.2.1 APPLICATION IDENTIFICATION 33
10.2.2 ESIGNATURE DETAILS 34
10.2.3 INTEROPERABILITY 36
10.2.4 MISCELLANEOUS 37
10.2.5 ASSESSMENT 37

10.3 OIL & GAS TRUST SCHEME 38
10.3.1 APPLICATION IDENTIFICATION 38
10.3.2 ESIGNATURE DETAILS 39
10.3.3 INTEROPERABILITY 42
10.3.4 MISCELLANEOUS 42
10.3.5 ASSESSMENT 42

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf
[RD8]	
[RD9]	

2 Glossary

2.1 Definitions

In the course of this Questionnaire, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

  It should be noted that for the purposes of this questionnaire, only services which rely on eSignatures are relevant, and that the focus is on eGovernment applications offered to citizens and businesses (A2C and A2B, rather than A2A).

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions. However, PKI solutions are the principal focus of this questionnaire, and non-PKI solutions should only be included if no PKI solutions are in common use. It should also be noted that the questionnaire only examines eGovernment applications in which the eSignature is used to sign a specific transaction, and not where the signature is merely used as a method of authentication of the eSignature holder as defined below.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[1].

[1] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

- *Authentication*: the corroboration of the claimed identity of an entity and a set of its observed attributes (i.e. the notion is used as a synonym of "entity authentication"). It should be noted that the questionnaire is focused on the use of eSignatures as a method of signing a transaction, and not on their use as a method for authenticating the eSignature holder.

- *Relying party*: any individual or organisation that acts in reliance on a certificate (in a PKI solution) or an eSignature.

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CRL ..... Certificate Revocation Lists

eID ..... Electronic Identity

OCSP ..... Online Certificate Status Protocol

PKI ..... Public Key Infrastructure

SCVP ..... Simple Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

TTP ..... Trusted Third Party

3 Introduction

3.1 eGovernment structure

The UK Government decided that rather than support multiple access channels being developed anew for each application as it became e-enabled, they would support the portal approach. The name of the portal is the "Government Gateway" and its external interface is as the website to use to register for online government services.

Thus the Government Gateway plays a major role in ensuring successful delivery of the UK's e-Government initiatives. Working with Government Gateway partners such as Microsoft, Dell, SchlumbergerSEMA and Cable and Wireless, the Office of the e-Envoy's e-Delivery team (as it was then – the OeE is now called the eGovernment Unit or eGU) launched the Gateway on the 25 January 2001 on time and to budget

Initially, a citizen or an organisation will register with the Government Gateway if to enrol for one or more government services (for example, Self Assessment, PAYE Internet Services for Employers and Electronic VAT Returns).

Then, once registered as a Government Gateway User, it is possible to:

- submit forms to government departments for the services for which you have enrolled. You will be able to carry out some services by filling in online forms on Government or private company websites. For other services, online forms will not be available and you will only be able to send forms by using software packages (such as payroll software);
- enrol for additional services as they become available;
- assign an Agent (such as your accountant or payroll bureau) to act on your behalf for any of the services you have enrolled for.

If registered as an organisation, it is also possible to:

- add other people within your organisation as Users of the Government Gateway. They will be able to carry out any of the services you have already enrolled for, and also enrol for new services. They will also be able to create and delete other Users;
- create Assistants who will have access to limited features within the Government Gateway, but can send your organisation's forms to the Government using appropriate software or websites;
- complete tasks such as deleting Users, changing the services that Users are assigned to and making changes to your registration details.

The portal can accept registration in two modes either with a User Id and password or with a digital certificate, however, once registered it is up to the specific application that the user enrols for that will determine whether a User Id/password is sufficient – some applications require a digital certificate. Where an application is satisfied with a User Id/password then it will also accept a digital certificate.

More detail on the technical solution presented by the Government Gateway is given in sections 5.1 and 10.1 below.

This portal-based approach means that for most Government Departments or agencies there is no need to be concerned with interoperability of digital certificates as the portal handles the authentication at login. It also means that there can be a simple policy for testing and accepting certificates from different CAs – they only need to test their compatibility to the portal and then provide access to all current or future applications that provide access via the Government Gateway.

In order to ensure that the CAs are managed properly and will not cause a risk of compromise to the process, the Government requires[2] that any third party providing registration services to support e-Government transactions must be approved under a scheme recognised by the UK government such as *tScheme*[3]. Note, this portal does not only give access to central Government applications but also devolved regional applications (e.g. for the Scottish Executive Environment & Rural Affairs Department) and local Government (e.g. Kings Lynn & West Norfolk council tax services).

However, there are two notable applications that do not use the portal (and they are both described in more detail below). The first is the e-Conveyancing application being developed for the Land Registry, which is a government executive agency and trading fund responsible to the Lord Chancellor that keeps and maintains the Land Register of England and Wales. Its main purpose is to register title to land and to record dealings once the land is registered. Established in 1862, it is required by statute to be self-financing and makes no call on public funds.

It was felt that the extreme sensitivity and liability implications relating to transactions for the buying and selling of people's homes meant that a bespoke solution needed to be developed that could be introduced carefully in phases with tight controls on all aspects of the process, and should thus not be added into the more generic solution provided by the Government Gateway.

The second such application is the DTI's Oil & Gas Trust Scheme. Here it was felt that the requirements of the industrial sector being served were more specific than those provided for by the Government Gateway's generic approach and that the financial model dictated by the value of the transactions meant that a standalone solution was the most efficient way of achieving a workable solution. Like the Government Gateway, *tScheme* is used as the basis for determining the suitability of the CAs but unlike it, there are extra requirements placed on the CA over and above the basic *tScheme* approval criteria. These cover items such as key size, use of Hardware Security Modules, specific content for some of the X.509 fields, etc.

With regard to e-Procurement applications, although the guidelines produced by the Office of Government Commerce are generic and can allow for the use of digital certificates, currently all of the implementations are based around Username and password authentication and do not require digital certificates and, therefore, are excluded form this study.

In order to ensure that all e-enabled applications can interoperate successfully, the UK Government has also spent a lot of time and effort in establishing a standards-based framework of standards and related XML schemas known as the e-Government Interoperability Framework (e-GIF)[4]. The e-GIF defines the technical policies and specifications governing information flows across government and the public sector. It covers interconnectivity, data integration, e-services access and content management.

[2] See http://www.cabinetoffice.gov.uk/csia/documents/pdf/RegAndAuthentn0209v3.pdf

[3] See http://www.tscheme.org

[4] See http://www.govtalk.gov.uk/schemasstandards/egif_document.asp?docnum=874

4 eGovernment and eSignature regulations

4.1 eSignatures regulatory framework

European Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures was transposed into UK legislation through:

- the Electronic Communications Act 2000, which came into force on 25th May 2000 and is in three parts:
  - part 1 concerns Certificate Service Providers and details the arrangements for registering providers of cryptography support services, such as electronic signature services and confidentiality services. However, the Government said that they would not commence this part of the act preferring to see the industry-led initiative, tScheme, carry out this function. On 25th May 2005, being the fifth anniversary of the day on which the Act was passed, having continued to be satisfied that tScheme meets the Government's objectives, part 1 effectively was repealed;
  - part 2 makes provision for the legal recognition of electronic signatures and the process under which they may be generated, communicated or verified. It will also facilitate the use of electronic communications or electronic storage of information, as an alternative to traditional means of communication or storage;
  - part 3 amends sections 12 and 46B of the Telecommunications Act 1984 and inserts a new section 12A into that Act. The new provisions are concerned with the modification of telecommunication licences otherwise than in pursuance of a reference to the Competition Commission. This Part also concerns matters such as general interpretation, the short title, commencement and territorial extent of this Act.

- The Electronic Signatures Regulations 2002, which came into force on 8 March 2002, these include provisions relating to the supervision of certification service providers, their liability in certain circumstances and data protection requirements concerning them. They also transpose verbatim Annexes I and II of the Directive to enable the meaning of the term "qualified certificate" to be understood as it is used in these Regulations.

4.2 eGovernment regulatory framework

As noted above, part 2 of the Electronic Communications Act 2000 covers the legal recognition of electronic signatures and, rather than make a definitive statement about their equivalence to handwritten signatures, section 8(1) of the Act, has given Ministers the authority to modify legislation to permit the use of electronic signatures as an acceptable alternative to a manuscript signature.

Whilst the act was being drafted, a written answer was put to Parliament indicating that eleven statutory instruments had already been identified that would create orders under Section 8 of the Act and then in its UK Online Annual Report 2000, the e_Envoy included a commitment by the Government to have implemented 70% (i.e. 8 out of the 11) by the end of 2001. Although, on 17 July 2001 the Government indicated that priorities might change as departments' e-business strategies evolved, and that while eight section 8 orders would be made by the end of 2001, they might not all be drawn from the original list.

However the Government's policy about updating the law to take account of new information and communication technologies developed further as a result of a combination of circumstances. These included experience of the use of electronic communications, a report by the Financial Law Panel (E-Commerce – Review of Legal Implications – Proof and Evidence) dated November 2000, and work done by the Law Commission in preparing an Advice to the Government[5] on e-commerce in the context of commercial transactions. This Advice includes the view (supported by the Financial Law Panel report) that, whilst each statutory requirement must be interpreted in context, in a neutral context an e-mail (and any attachment) will already satisfy a statutory writing requirement, at least if visible, without requiring specific provision via a Section 8 order. The Advice observes that a specific statutory context may make it clear that a requirement cannot be satisfied electronically and that there may be some contexts where the requirements are capable of being satisfied electronically but, for reasons such as public policy, it may be desirable to impose an electronic form requirement where none currently exists.

The implication of this Advice is that not all statutory references to 'writing' (currently estimated at over 40,000) need to be updated to permit the use of electronic communication. This is contrary to the pre-dominant views expressed in the public consultations which informed the drafting of the Electronic Communications Act 2000, in which the broad pattern of response from industry and legal experts was that there was sufficient doubt about the legal admissibility of all forms of "electronic writing" to require clarification on a case by case basis.

In addition departments have had to consider whether in the absence of a policy, legal or practical reason to make specific provision for electronic communication, the better option is to leave the law unamended and concentrate on matters such as delivery or system integrity. To amend the law without good reason could have the effect of casting doubt on the legality of using electronic equivalents to meet requirements that are not or have not been updated but which present no barrier, in principle, to electronic ways of working.

As a result about 400 pieces of legislation were identified that might need to be subject to an order under section 8, but it is difficult to ascertain how many of these have been laid before parliament. This is mainly for the following reasons:

1. Each department or agency is responsible for its own legislation, so there is no central coordination of this activity;
2. The titles chosen for the Orders do not follow any clear naming convention so it is not possible to do a simple search of parliamentary publications, although very often the convention followed is "<name of primary legislation> (<short phrase – usually containing word 'electronic'>) Order <year>", e.g. "Companies Act 1985 (electronic communications) Order 2000";
3. Sometimes a number of pieces of primary legislation are amended under a single statutory instrument, e.g. The Transport Security (Electronic Communications) Order 2006 that covers five separate enactments;
4. Some amendments are made using similar powers contained in the Finance Act 1999, e.g. the ability to allow the filing of personal tax returns to Her Majesty's Revenue & Customs department.

[5] See http://www.lawcom.gov.uk/docs/e-commerce.pdf

5 eGovernment applications using electronic signatures

5.1 Government Gateway

All answers to the questionnaire can be found at section 10.1.

5.1.1 Application identification

In 1999, the UK Government commissioned a report from PA Consulting looking at the cross-government infrastructure that would be required to enable the delivery of online services and joined-up government to be implemented. One of the recommendations in that report was that the UK Government should procure a central 'gateway' that would help tackle common issues such as user identity management, messaging and transaction handling. The result of that report was an EU procurement run by the Cabinet Office that produced the Government Gateway.

The Government Gateway is an important part of delivering joined-up government, using a set of components that provide Authentication, Transaction routing and reliable messaging. It enables citizens, businesses, intermediaries and even other government organisations to communicate with the Government from a single point of entry. These form part of the services required for ensuring delivery of the Prime Minister's commitment that by 2005, 100% of government services should be available electronically.

These products, provided by the e-Delivery Team (EDT) on behalf of the UK Government, are designed to facilitate the efficient provision of on-line services in a cost-effective manner. They enable government organisations to focus on the rapid delivery of on-line services, rather than in building time and time again the common underlying components required for on-line services in the UK.

5.1.2 eSignature details

5.1.2.1 Legal Aspects

Depending on the service being provided, if it is covered by legislation then an assessment will need to be done by the relevant government department as to whether electronic data can be utilised and whether an electronic signature is valid. If not, an order will need to be laid before parliament to amend the legislation appropriately. See 4.2 above.

5.1.2.2 Technical Aspects

The Government Gateway consists of a set of centrally hosted and managed hardware and software that provides the Government Gateway User Interface (www.gateway.gov.uk); the underlying user identity management services and interfaces; and a middleware XML hub that provides the messaging services that link together front- and back-end systems. It provides a single, reliable, secure and consistent route for secure, authenticated messages into and out of customer backend systems

There are four key components to the system:

- **Registration and Enrolment.** A facility that supports both User ID/Password and Digital Certificate authentication methods. This enables end-users (citizen, organisations and intermediaries) to have single sign-on facilities across all government services – national, regional and local. The Soap API can be used to develop an interface to this component.
- **Authentication and Authorisation.** This allows the portal to effect a user logon, using the Government Gateway as the authentication source. The applicant's Government Gateway

user ID is supplied along with their clear-text password, unless they have registered with the Government Gateway using a digital certificate in which case a signed version of the X.509 certificate is presented instead. This can be implemented via a SOAP API if required.

- **Transaction Engine.** Documents and business forms can be exchanged reliably between government, intermediaries, citizens and external organisations. This provides an electronic interface to the Internet that enables electronic forms and requests to be submitted to government. It does not have a user interface, but works through a clearly defined submission protocol involving the exchange of XML documents.
- **Payment Engine.** A payment facility that enables users to make payments to government organisations by means of credit cards and debit cards. The payment facility also supports the issuing of direct debit instructions.

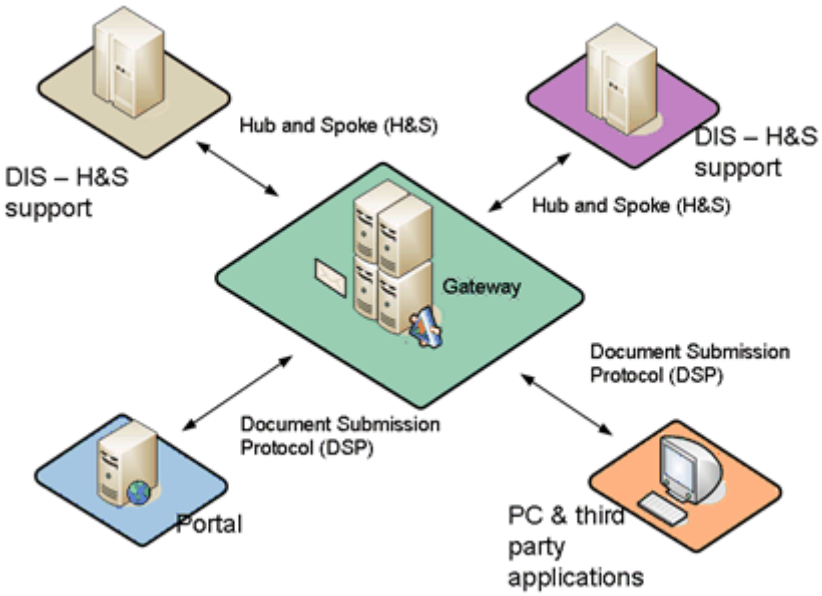
The key to providing an effective shared service is in the enrolment process whereby a registered user of the Government Gateway can enrol for a new service and be uniquely identified to that service without having to re-enter all their basic data again, this is done by utilising the concept of Known Facts. A Known Fact is a piece of data, held by a government department or local authority, that, when combined with other Known Facts, can be used to identify a citizen or organisation. For example, the Inland Revenue can uniquely identify a citizen from a combination of their Unique Tax Reference (UTR) and National Insurance number (NiNo) or Postcode.

Known Facts are used by the Government Gateway to enrol a user for a particular service. Each service has its own set of Known Facts that a prospective user must supply before they can be enrolled to use the service. For example, a user must provide their UTR and either their NiNo or their Postcode successfully for the Inland Revenue's Self Assessment service1. When entered by the user these Known Facts are then checked to ensure that they match the Known Facts provided by the customer. Customers providing services through the Government Gateway supply a set of these Known Facts data for each service where they need the users to be verified against existing data. They also provide ongoing updates to this data either electronically (via the 1.6.5 SOAP API or customer generated admin messages), or manually (via CD upload).

5.1.2.3 Organisational Aspects

In order for service owners to communicate with the Government Gateway they need a "DIS", which stands for "Departmental Integration Server". It provides a reliable two-way messaging endpoint for Gateway/service owner interactions, as well as handling a wide variety of administration messages associated with running online services. In effect it is the entry point for backend systems to make use of the Government Gateway's messaging and authentication services. In addition, many DIS vendors also provide a range of comprehensive complementary features, such as backend integration with existing applications and technologies and business processing rules and execution.

Hub and spoke refers to a messaging mechanism that enables DIS systems to communicate with each other through the Transaction Engine. So organisation A can send messages to organisation B. One DIS installation thus not only provides access to the messaging and authentication features of the Government Gateway to support interactions with businesses, citizens and intermediaries, but the same infrastructure also provides government-to-government messaging.



"DSP" stands for the "Document Submission Protocol". This is the standard method by which third party application software submits documents and transactions into the Government Gateway for onward delivery to the intended recipient.

5.1.3 Interoperability

Although the Government Gateway uses Microsoft technology internally, it exposes all of its functionality through e-GIF compliant open standards. These include Web services, XML, HTTP and SOAP, which are natively supported open standards of the Microsoft products used. A wide range of systems have interoperated with the Government Gateway since its launch, including systems running Sun's J2EE technology, IBM technologies, Apache, Tomcat and other technologies and applications including standalone PC application software. The Government Gateway is widely regarded as the best example of an e-GIF compliant project currently operating in UK government.

The Government Gateway uses standards such as WS-Security, which is an open standard agreed by OASIS and supported across a wide variety of competing vendors (such as BEA, Sun, IBM and Microsoft). The use of such open standards ensures that it is as easy as possible to integrate with the Government Gateway's services from whatever platform may be in use. It is true that the original application, launched in 2001, used a bespoke 'A-ticket' mechanism: this was because at that time there was no agreed industry standard that could be adopted. So the Cabinet Office agreed with the various users of the Government Gateway a local UK Government standard that would provide the authentication mechanisms required. This old method is being end-of-life'd in 2006 in recognition of the fact that WS-Security and related standards now provide the necessary functionality, meaning that the old UK government-specific mechanism is no longer required or desirable.

5.1.4 Miscellaneous

Although there are no statistics relating specifically to use of electronic signatures, between February 2001 and June 2005 there were over 6.8 million active enrolments. In the two years to June 2005 there were more than 12.1 million SOAP authentications and in the period from October 2003 to June 2005 there were 152,000 settled transactions totalling over £5.9 million.

5.1.5 Assessment

Every service that provides access via the Government Gateway must do a risk analysis and business impact analysis to decide what level of authentication is appropriate. This then determines whether access can be via User Id & password or digital certificate. However, digital certificates need to be purchased by users and this cost can provide a significant dis-incentive, so it is not uncommon for service providers to implement extra risk-mitigation measures in order to allow the use of User Id & password. As a result the take-up of digital certificates is a lot less than was originally envisaged.

5.2 e-Conveyancing

All answers to the questionnaire can be found at section 10.2.

5.2.1 Application identification

Ideas for re-engineering the conveyancing process in England and Wales have been developing over a number of years. In 1998, preliminary proposals were set out in the joint report by the Law Commission and Land Registry entitled *Land Registration for the Twenty First Century* (Law Com 254).

5.2.2 eSignature details

5.2.2.1 Legal Aspects

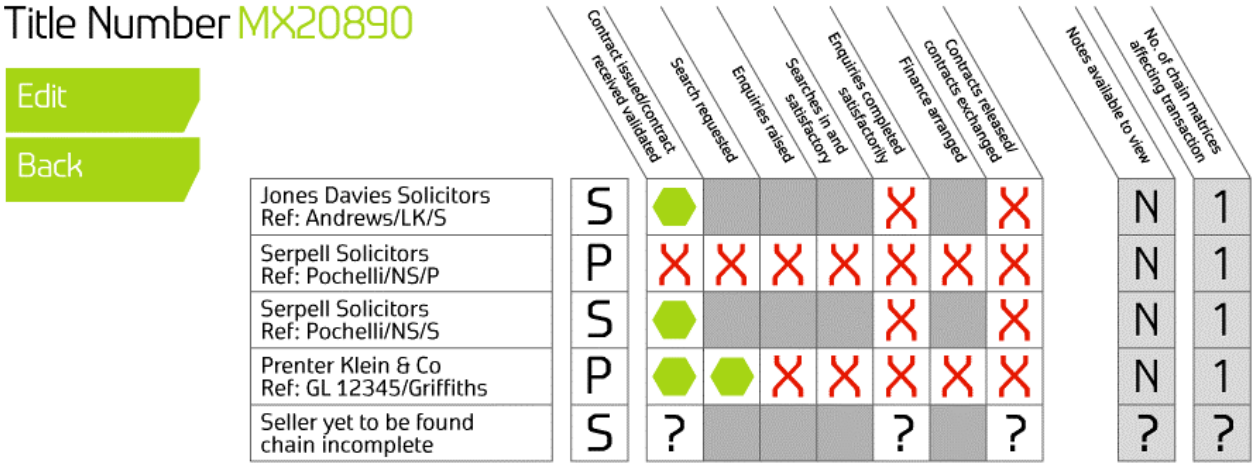
The Land Registration Act 2002 contains the legislative provisions to enable the implementation of e-conveyancing services. Secondary legislation in the form of rules now needs to be drafted and passed by Parliament to give effect to those legislative provisions.

5.2.2.2 Technical Aspects

The process will comprise a certain amount of re-engineering and is expected to incorporate the following new features:

- At the time the seller's conveyancer uses the e-conveyancing service to transmit the draft contract from their computer to the buyer's conveyancer, automatic validation checks will compare contract data with Land Registry data and electronic messages will indicate any discrepancies and/or omissions. It is anticipated that these will be resolved online. At this time, a new "notional" register will be built on the system indicating, as each document is prepared, what the new register would look like.

- Conveyancers will also record on the system the stage reached on each transaction by adding data to a "chain matrix" available in the central service. This will enable conveyancers and Land Registry to see the progress of all the transactions linked together in a chain. Chains will therefore become more transparent. The conveyancer's task in synchronising exchange and completion dates should be simplified, with any blockage points being immediately identifiable to facilitate enquiries. An example of how a chain matrix might look is set out below. This is the subject of ongoing consultation and may change as a result of this.



An example of how a chain matrix might look

- There will also be a facility for conveyancers to view Land Registry's day list (a log of all pending applications) prior to exchange of contracts, in order to ascertain whether or not there is such an application which may adversely affect the transaction - for example a bankruptcy notice.

- At the contract stage, there will be an electronic equivalent of contracts. Contracts will be exchanged electronically when the buyer's and seller's conveyancers have signalled that agreement has been reached and contracts have been signed and released for electronic exchange. The central service will provide for automatic exchange of contracts relating to all transactions in a property chain. For this and other purposes, conveyancers will need to have electronic signatures. Land Registry has initiated a project to determine an effective and affordable e-signature ("document authentication") solution. Payment of deposits on exchange will be accounted for in the central service and paid by the EFT service.

- A substantive register entry will be made to note the contract. This would also provide, automatically, a priority protection period in respect of any competing application and during which completion with registration would normally be expected to take place. Provision to extend the priority protection period may be necessary for delayed completion.

- During this period the draft electronic transfer and any draft electronic legal charges will be agreed and finalised. These documents will then be signed electronically in anticipation of completion just as they are in the existing paper system. Shortly before completion the parties to the transaction (and all parties in the chain) will signal their readiness to complete in accordance with the terms of the contract. They will do so by using an extension of the chain matrix, which will indicate firstly that all necessary documentation is signed and, secondly, that all the financial arrangements are in place.

- Registration will take place with completion. The changes signalled in the notional register will be verified and the new edition of the register will be finalised.

- All financial obligations, including Stamp Duty Land Tax and Land Registry fees as well as payments between buyers, sellers, lenders and conveyancers, will be settled through the EFT service. With the help of e-technologies, the amounts of Stamp Duty Land Tax and Land Registry fees will be correct in virtually all cases. This will contrast with the present high incidence of errors.

- Post-completion - it is envisaged that no further action would be needed for transfers relating to registered land. When the purchase of unregistered land is included in a chain of transactions, it will only be possible to achieve simultaneous completion and conditional registration for that transaction. The reason for this is that the unregistered title needs to be examined by Land Registry.

5.2.2.3 Organisational Aspects

There are four key groups of professional stakeholders affected by the introduction of e-conveyancing. The legal and financial services sectors are the largest groups although the property-marketing sector is also very significant. There are also a number of other government departments with which e-conveyancing services will need to interface. It is estimated that there are over two hundred thousand professional stakeholders and so, a range of proposed services for all have been developed.

With home ownership now standing at over 70%, information services for the public will also be an important element of e-conveyancing.

5.2.3 Miscellaneous

With the world's largest property database of over 20 million titles, Land Registry underpins the economy by guaranteeing ownership of many billions of pounds worth of property. Around £1million worth of property is processed every minute in England and Wales.

It is envisaged that the CA will need to be scaled to handle potential volumes in excess of 400,000 transactions per month.

5.2.4 Assessment

The principal electronic signature part of the application is in the Document Authentication element, which was prototyped after the procurement of an Entrust PKI solution on 27th September 2004. The first e-signature was created on 22nd August 2005 and the project was formally closed on 30th November 2005. A full evaluation report of the experience of using electronic signatures in this prototype is available on the Land Registry website[6].

Baroness Ashton of Upholland, Parliamentary Under Secretary of State for Constitutional Affairs, has given the go-ahead for Land Registry to launch its e-conveyancing pilot service (the system to be used for domestic sales) in October 2007.

5.3 Oil & Gas Trust Scheme

All answers to the questionnaire can be found at section 10.3.

5.3.1 Application identification

In line with UK Government targets, DTI are delivering most of their services digitally through the UK oil portal. DTI started issuing digitally signed chemical permits in January 2005. Decommissioning notices followed in July 2006. During 2006/07 DTI will begin to require certain transactions to be delivered digitally signed. Licence Round applications[7] and Produced Water Trading are the first two such areas.

---

[6] See http://www.landregistry.gov.uk/assets/library/documents/evaluation_report_version_1.2_sb.pdf

[7] See http://www.og.dti.gov.uk/consultations/e_licences.pdf

DTI have worked with BP, Exxon, Shell and UKOOA to deliver a solution to this. The oil company interest was not only to enable them to satisfy regulatory requirements but also because they all had formative plans to move to PKI internally and were looking for a stimulus to externalise their plans.

In the course of the work DTI ran an industry consultation. The responses to this were all positive. The themes that emerged in the responses were that any solution must be low cost, easy to use, not UK centric and based on standards.

Following the consultation DTI ran a series of pilots with a number of companies and formulated the Oil & Gas Trust Scheme (OGTS) and produced a set of Trust Rules that defined a set of standards for the issue and use of digital certificates for use in regulatory work in the UK. The view was that these Trust Rules, which were based upon emerging international standards, would have wider applicability in the global oil industry.

5.3.2 eSignature details

5.3.2.1 Legal Aspects

None.

5.3.2.2 Technical Aspects

There are three key principles that shaped the technical solution:

1. Rigorous registration process - in keeping with best-practice and UK government requirements, emphasis has been placed on verifying the identities of individuals within corporate organizations. This is in accordance with HMGVind[8] and HMGVorg[9], Level 2.
2. Software keys are sufficient - this ruleset recognises that keys held in software (i.e. not on a smart card) where there is adequate corporate protection policy and practices relating to the computer carrying the keys, are sufficient for all low to medium risk business transactions.
3. tScheme Approval with self-assessment for additional requirements - tScheme Approval (or equivalence)[10] will be used as the minimum standard for all TSPs. The ruleset also imposes a small number of additional requirements, to form a common industry specific layer, which will be self-assessed by the TSP.

These additional requirements include:

- All Keys must have a Key length of at least 1024 bits, this relates to both end-user keys and keys in operation at the CA;
- TSPs must generate their CA Key Pairs in hardware certified to at least FIPS 140-1 level 3;
- CA Signing Keys must not exist in plain text outside of the HSM;
- Where keys are held in software, adequate organisation policies and practices must be in place to protect the security of keys such that only the authorised or intended user can gain access to the keys;
- TSPs shall include the fields specified in the table below in end-entity certificates;

[8] See http://www.cabinetoffice.gov.uk/csia/documents/pdf/HMG_reqmnt_veri_ID_individual.pdf

[9] See http://www.cabinetoffice.gov.uk/csia/documents/pdf/HMG_reqmnt_veri_ID_org.pdf

[10] TSPs domiciled outside the UK that have achieved the WebTrust Seal Of Assurance will, for the purposes of the Oil & Gas Trust Scheme, be deemed to be tScheme equivalent.

- "Subject – Organisation" should be the company name as registered at Companies House;
- "Subject – Organisation Unit" should hold an additional indicator (OGTS) after the entry to identify that the certificate has been issued in accordance with the Oil and Gas Trust Scheme, e.g. DTI (OGTS);
- Dates should be displayed according to eGIF standards;
- TSPs should avoid setting extension fields to critical to prevent rejection of the certificate by the relying party;
- A TSP must make its root and intermediary certificates available to all parties in the Oil and Gas Community of Trust;
- A TSP must publish a CRL. The CRL must be issued at least once in any 24 hour period. Additionally an OCSP service may be provided;
- Where an OCSP service is provided it must be made available 24x7[11];
- Where an OCSP service is provided it must allow unsigned requests for certificate status or an alternative mechanism provided at reasonable cost for applications to make OCSP calls to validate those certificates.

Field Name	Description
Version (1, 2 or 3)	The version of the X.509 certificate.
Serial number	Uniquely defines certificate issued by the certificate authority.
Issuer	Identifies the CA that issued certificate. The Distinguished Name (DN) has the following components: CN - Common Name (**mandatory**) O - Organisation (**mandatory**) OU - Organisation Unit (**mandatory**) L - Location (**optional**) C - Country (**mandatory**) E - Email (**optional**) S - State (**optional**)
Subject	Information about certificate owner. The Distinguished Name (DN) has the following components: CN - Common Name (**mandatory**) O - Organisation (**mandatory**) OU - Organisation Unit (**mandatory**) L - Location (**optional**) C - Country (**mandatory**)

[11] This means that the general service hours for the OCSP service are 24 hours a day, seven days a week, and it allows for scheduled and emergency outages in accordance with the TSP's SLA.

	E - Email (**optional**) S - State (**optional**)
Valid from	Start date of certificate period of validity.
Valid to	Ending date of certificate period of validity.
Subject Public Key Info	The subjects public key (1024 bits).
Issuer Unique ID	Uniquely identifies the issuer.
Subject Unique ID	Uniquely identifies the subject.
Signature Algorithm	Contains the identifier for the cryptographic algorithm used by the CA to sign this certificate.
Signature Value	CA signature to confirm certificate validity and authenticity.

5.3.2.3 Organisational Aspects

The OGTS interface to the UK Government is the responsibility of the Licensing and Consents Unit within the Oil and Gas Directorate of the DTI.

5.3.3 Interoperability

The expectation is that the restriction put on the contents of the X.509 certificate will ensure interoperability between the DTI and any of the approved CAs. However, it does mean that it is unlikely that the certificates will be useful with any other eGovernment application.

5.3.4 Miscellaneous

The Application has been used in all licences and consents issued in 2006 (between 1000 and 5000).

5.3.5 Assessment

This has been a very tightly focused project with a clear and restricted target and, as such, has achieved its aims.

6 General Assessment

By deciding upon the portal approach for access to eGovernment services, the UK has been able to implement a wide, and growing, range of services to the public and to commercial organisations without having to expend repeated effort in getting the identity management piece implemented.

By this means also, if (or when) the Government implements an eID card it will be relatively straightforward to make use of it in providing access to all of the services that are available via the Government Gateway.

As far as the legal situation is concerned, the ability to use the Section 8 orders under the Electronic Communications Act 2000 as the means for amending primary legislation by the use of statutory instruments, which can more easily and efficiently be drawn up, has allowed a flexible and priority-driven approach to be taken as to when and how specific changes are needed to allow electronic communications and electronic signatures to have full legal effect, equivalent to handwritten signatures.

Finally, with regard to internal and external interoperability: internal interoperability is not an issue because certificates are either targeted at specific applications like e-Conveyancing or the DTI OGTS and thus not designed nor required to interoperate, or they are targeted at the Government Gateway, in which case there is no other relevant application to need to interoperate with.

External interoperability should not be an issue per se for the Government Gateway as there is no requirement for UK specific data to be included in the certificate. Therefore provided the external certificate does not itself include data that is incompatible with the Gateway, there is no reason to presume that there would be any interoperability issues.

7 Operational and planned applications

Interesting applications mentioned in the tables below have been further elaborated above with information on the actual usage of the applications. It should be noted that the list is not exhaustive.

7.1 Applications at the national level

	Application	Scope	Reference	Contact	Signature
1.	Government Gateway	Online access to Government services for citizens and businesses	http://www.gateway.gov.uk/	Paul.kilner@cabinet-office.x.gsi.gov.uk	Simple certificate
2.	eConveyancing	An electronic system of conveyancing that makes buying and selling houses easier for the general public, conveyancing professionals, and other parties involved in the process	http://www.landregistry.gov.uk/e-conveyancing/	darrell.peart@landregistry.gsi.gov.uk	Simple certificate
3.	Oil & Gas Trust Scheme	Allow the UK Oil Industry to apply for and receive consent or other information electronically	http://www.logic-oil.com/ogts/	stewart.robinson@dti.gsi.gov.uk	Simple certificate

8 Annex A: Contact details of National Correspondents

Contact Information of the person(s) completing the questionnaire. The person(s) will be contacted for any queries related to this questionnaire.

8.1 Primary Contact

Country	United Kingdom
Name	Richard Trevorah
Organisation	xidm Limited

8.2 Alternative Contact

None

9 Annex B: National Regulations Details

National correspondents are required to include references to the legal sources that they have consulted. This includes references to laws, other regulations, and doctrine, in such a manner that a legal expert with knowledge of the national legal system would be able to retrieve the sources.

Whenever referring to national regulations or institutions, the correspondents are required to provide the local name as well as an English language translation of the regulation's title.

If available, links to on-line resources (legislation, judicial decisions, governmental websites, and professional organisations) should be included.

National regulation title	National regulation translated title (English title)	Relevant links to on-line resources
Electronic Communications Act 2000		http://www.opsi.gov.uk/acts/acts2000/20000007.htm
The Electronic Signatures Regulations 2002		http://www.opsi.gov.uk/si/si2002/20020318.htm
Land Registration Act 2002		http://www.opsi.gov.uk/acts/acts2002/20020009.htm

10 Annex C: Application questionnaires

10.1 Government Gateway

10.1.1 Application identification

Application/Service Classification	
Application/Service Name	*Government Gateway*
Application/Service Type	*A2B or A2C*
Concerned sector	*Potentially all aspects of electronic access to Central, Regional and Local Government for citizens and businesses*
Application/Service Cross-Border Type	*None, it is targeted at provision of access to UK e-Government applications for UK citizens and businesses*
Level of Online Sophistication Type	*Stage 4 (Transaction: full case handling, decision and delivery)*
Intended "clients"	*Any natural or legal person (or their agent) who requires access to supported application e.g. personal income tax, company VAT, etc*
Abstract Description	*The Government Gateway allows secure authenticated transactions and joined-up government services to take place via the web. The Government Gateway is an authentication and routing engine built on open standards, allowing different systems in different government departments to communicate with the Government Gateway and with each other. This means that in the future, electronic transactions involving many different departments at once will be possible, ensuring a truly joined-up electronic public service.* *Over time it is anticipated that the Government Gateway will handle a substantial part of the estimated 5-6 billion of annual government-related transactions. As part of the UK's Critical National Infrastructure, the Government Gateway provides a highly secure environment, a resilient 'always on' service and the capacity to handle high volumes.*
Identification of Application/Service Entities	*The main entities are the users (or their agents) requiring access to e-Government services, the e-Delivery Team (who maintain and develop the Government Gateway infrastructure) and the various government departments providing the e-Services*

Procedural Details	*Applicants are either given a UserID and password or they buy a digital certificate from an approved supplier, which they then register with the Government Gateway, to allow access to services. Users then enrol for specific services. Depending on the Authentication level required by the service, access can be by UserID/Password or certificate, or (where higher security is required) by certificate alone*
Current status	*The Government Gateway went live in 2001. The Government Gateway has 9 million active enrolments (of which 20,000 are certificates) with more than 100 enabled services from 50 different government entities*
Expected future developments	*Throughout 2006/7 EDT will be working with a number of central and local government departments to implement an additional 50–100 services on the Gateway, making it truly the centre piece of UK government's joined–up initiatives*

Responsible Organisation	
Organisation Name	*The e-Delivery Team is part of the Cabinet Office's e-Government Unit*
Organisation Type	*National*
Date of interview	*26th October 2006*

Application/Service System Details	
Communications Information	*Internet*
External interface	*Web portal at http://www.gateway.gov.uk/*
Data structures processed by the application	*Portal permits the completion of electronic forms interactively on the Internet, while services permit the completion of electronic forms locally on a PC. In both cases the Internet and the Government Gateway provide the mechanism for the submission of completed forms to the appropriate organisation and the return of a corresponding receipt acknowledgement.*

10.1.2 eSignature details

Legal aspects	
Does the system rely on a simple / advanced / qualified / other signature?	*UserID and Password or Simple signature*
Is the signature required/recommended?	*Required for some services on basis of risk analysis*
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	*No change in strategy planned with regard to authentication and enrolment procedures*
What is the legal basis (law, decree,…) for this application?	*No legal basis required for the portal, only potentially for the particular application*
How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?	*Liability with regard to use of certificate is covered by contract between user and issuing CA, all other liability is covered as per normal rules for government processes*

Technical aspects	
What are the parties involved in the signature process?	*The user applies to one of the approved certificate suppliers, currently they are ChamberSimplySign and Equifax. This certificate is then used to register with the Government Gateway*
What kind of token or credentials are used (smart cards, software certificates, paper tokens …)?	*Software certificates*
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	*None*
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	*Windows 95 or NT 4 (SP3) or higher with Internet Explorer 5.01 or above*
What information is signed by the user and what is the objective of the signature?	*The signature is initially used to authenticate the user to the Gateway. Subsequent transaction data is signed by the user and verified by the Gateway before being passed to*

	the service application
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	*No*
What are the relevant policies (CPS, certificate policy, signature policy)?	*As published on the websites of the approved CAs*
How are the signature/certificate presented to the application?	*Via the web portal by utilising the Cryptographic Services module in the OS of the user's PC*
What information is included in the certificate, and what is the role of this information in the functioning of the application?	*No Gateway specific information is included in the certificate*
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)? If yes, describe the framework in the country general profile. If no, specify which standards have been implemented in the eSignatures application? Depending on the signature type, this may include standards regarding certificates, signature formats, signature algorithms, token formats, other information security standards, etc.	*No existing generic eSignature framework - Certificates must comply with X.509*
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	*The signature is verified at the point of logging-in to the portal and, at the same time, the certificate chain is checked for validity to its root*
What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP…)	*CRL*
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	*The certificate plus evidence of successful verification and validation is secured in the system audit trail at log-in*

Organisational aspects	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	*The certificate suppliers must be approved under a scheme recognised by the UK Government such as tScheme (www.tscheme.org), currently they are ChamberSimplySign and Equifax*
Who are the relying parties[12]? Describe the context?	*The Government Gateway relies on the certificate as a means to authenticate the user*
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	*The certificate suppliers must be approved under a scheme recognised by the UK Government such as tScheme (www.tscheme.org), currently they are ChamberSimplySign and Equifax*
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	*Validity period is up to three (3) years, conditions for suspension or revocation are detailed in the certificate policies (CP) for the relevant CA*

10.1.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	*Anyone can register with the Gateway but enrolment with services would depend on entitlement to the service and not on basis of nationality per se*
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	*None*

[12] « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

10.1.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	*None relating specifically to use of electronic signatures*
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	*None*
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	*No*

10.1.5 Assessment

Assessment	
Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses). Take this opportunity to bring any fruitful information that was not addressed by previous questions.	

10.2 e-Conveyancing

10.2.1 Application identification

Application/Service Classification	
Application/Service Name	*e-Conveyancing*
Application/Service Type	*A2B and A2C*
Concerned sector	*Transfer of ownership of land and property*
Application/Service Cross-Border Type	*None*
Level of Online Sophistication Type	*Stage 4 (Transaction: full case handling, decision and delivery)*
Intended “clients”	*Conveyancers representing the parties involved, lenders and individuals doing their own conveyancing*
Abstract Description	*Our mission is to "make conveyancing easier for all" - specifically, to develop an electronic system of conveyancing that makes buying and selling houses easier for the general public, conveyancing professionals, and other parties involved in the process*
Identification of Application/Service Entities	*Home owners (buyers and sellers), Lenders, Conveyancers and Estate Agents*
Procedural Details	*Authentication, signature and encryption using Public Key Cryptography to secure communications and transactions at all stages in the process (including electronic funds transfer) relating to transfer of ownership of property covered by the Land Registration Act 2002*
Current status	*Phased implementation in process of elements in the supply and presentation of data relating to the conveyancing process*
Expected future developments	*Pilot of e-Conveyancing system scheduled for October 2007*

Responsible Organisation	
Organisation Name	*Land Registry*
Organisation Type	*National*
Date of interview	*27th October 2006*

Application/Service System Details	
Communications Information	*Access to the system will be by Direct Link, Channel Access, Internet and Service Interfaces*
External interface	*Web portal at http://portal.landregistry.gov.uk*
Data structures processed by the application	*Secure access to stored documents, maps etc. Secure exchange of contracts containing XML data and other messages relating to progress in the transfer process*

10.2.2 eSignature details

Legal aspects	
Does the system rely on a simple / advanced / qualified / other signature?	*Simple*
Is the signature required/recommended?	*Required*
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	*No plans at present to change type of signature*
What is the legal basis (law, decree,…) for this application?	*Land Registration Act 2002 (http://www.opsi.gov.uk/acts/acts2002/20020009.htm)*
How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?	*The Agency should maintain liability if the system security is breached, unless the conveyancer is negligent or fraudulent*

Technical aspects	
What are the parties involved in the signature process?	*Land Registry will act as the CA and will interface directly to users requiring certificates*
What kind of token or credentials are used (smart cards, software certificates, paper tokens …)?	*Software certificates*
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of	*None*

eSignature?	
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	*Not specified*
What information is signed by the user and what is the objective of the signature?	*All important documents, messages and data will be signed to ensure integrity, authenticity and non-repudiation*
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	*No*
What are the relevant policies (CPS, certificate policy, signature policy)?	*Not yet finalised*
How are the signature/certificate presented to the application?	*Not yet finalised*
What information is included in the certificate, and what is the role of this information in the functioning of the application?	*Not yet finalised*
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)? If yes, describe the framework in the country general profile. If no, specify which standards have been implemented in the eSignatures application? Depending on the signature type, this may include standards regarding certificates, signature formats, signature algorithms, token formats, other information security standards, etc.	*No existing generic eSignature framework - Certificates must comply with X.509*
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	*Not yet finalised*
What types of validation protocols are used for the electronic certificate	*Not yet finalised*

validation? (OCSP, CRLs, SCVP…)	
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	*Not yet finalised*

Organisational aspects	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	*Land Registry will also be the CA and is building its own PKI*
Who are the relying parties[13]? Describe the context?	*All parties to the conveyancing process*
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	*Land Registry CA will issue/maintain credentials, but issuance procedure not yet finalised*
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	*Not yet finalised*

10.2.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	*Nationality of participants to a conveyancing transaction is not an issue, however, details of registration process for non-UK nationals not yet finalised*
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	*Interoperability with certificates from any other CAs not currently envisaged*

[13] « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

10.2.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	*N/A*
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	*Still under development, pending pilot in October 2007*
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	*No specific Government initiatives relating to e-Conveyancing at this time*

10.2.5 Assessment

Assessment	
Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses). Take this opportunity to bring any fruitful information that was not addressed by previous questions.	

10.3 Oil & Gas Trust Scheme

10.3.1 Application identification

Application/Service Classification	
Application/Service Name	*Oil & Gas Trust Scheme*
Application/Service Type	*A2B*
Concerned sector	*North Sea Oil & Gas operating companies*
Application/Service Cross-Border Type	*Borders not relevant, when Shell use a certificate it is irrelevant whether they are signing the message in the Netherlands or in the UK*
Level of Online Sophistication Type	*Stage 3: Two-way Interaction: Processing of forms including digitally signed data*
Intended “clients”	*Oil & Gas companies operating on the United Kingdom Continental Shelf*
Abstract Description	*Establishing a technical infrastructure that will deliver, accept and store all (digitally signed) North Sea consents and notices. Two major requirements in establishing this infrastructure is to ensure that all communications are confidential and secure and that the result of the process satisfies the PD 0008:1999 for Legal Admissibility of Evidence*
Identification of Application/Service Entities	*The DTI and the Oil & Gas companies operating on the United Kingdom Continental Shelf*
Procedural Details	*At the DTI:* • *All applications and related subsequent submissions will eventually be electronic and deployed through the UK Oil Portal authenticated by a digital signature.* • *Final consents and notices, the "digital documents" will be sent and signed electronically from the UK Oil Portal on behalf of the Secretary of State.* • *There will be no hard copy of these produced by the DTI.* • *The "digital documents" will be held in a PD 0008:1999 approved document management system.* • *The "digital documents" held by the DTI will be regarded as the master set.* • *Access to the master "digital documents" will be provided to Oil Companies at any time.* *At Oil company:* • *Oil companies will eventually assign digital signatures*

	to sections involved in consents and approvals. • *All communication will be electronic.* • *Final consents and notices will be received in electronic form, digitally signed.* • *The digitally signed documents may be stored internally.*
Current status	*Oil & Gas Trust Scheme is operational with 5 approved suppliers of digital certificates*
Expected future developments	*Working with industry to see whether concept can be rolled out to other business areas*

Responsible Organisation	
Organisation Name	*The Licensing and Consents Unit of the DTI*
Organisation Type	*National*
Date of interview	*27th October 2006*

Application/Service System Details	
Communications Information	*Documents created on web via portal or created offline, digitally signed and then emailed over the internet*
External interface	*Web portal at http://www.og.dti.gov.uk/portal.htm*
Data structures processed by the application	*Varies, some are fixed format based on XML some are free format.*

10.3.2 eSignature details

Legal aspects	
Does the system rely on a simple / advanced / qualified / other signature?	*Simple*
Is the signature required/recommended?	*It depends on the form/document, some forms can be created via the portal (using Username/Password) whereas some must be digitally signed and emailed*
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	*Future strategy is to allow for Licences to be digitally counter-signed by multiple parties and to allow for digital signing of web-based forms*

What is the legal basis (law, decree,…) for this application?	*N/A*
How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?	*Existing contractual arrangements will apply*

Technical aspects	
What are the parties involved in the signature process?	*Parties either purchase certificates from approved CAs or use certificates from an approved internal CA*
What kind of token or credentials are used (smart cards, software certificates, paper tokens …)?	*Not specified by the application – they can either be software certificates or stored on smart card or USB token depending on the CA*
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	*As per type of certificate identified by previous answer*
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	*Either an appropriate version of Adobe Acrobat that supports digital signing or use of signing utility provided by DTI to members of the scheme*
What information is signed by the user and what is the objective of the signature?	*The data required to complete consents and notices is signed to ensure authentication, integrity and non-repudiability*
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	*Not yet but planned for future*
What are the relevant policies (CPS, certificate policy, signature policy)?	*No requirements from scheme, policies are defined by the approved CAs*
How are the signature/certificate presented to the application?	*Either as signed XML or signed pdf, with a copy of the certificate attached for verification and validation*
What information is included in the certificate, and what is the role of this information in the functioning of the application?	*The critical items are the public key to allow signature verification and the reference to the issuing CA to allow path validation to a recognised Root CA*
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed	*No existing generic eSignature framework - Certificates must comply with X.509*

standards)? If yes, describe the framework in the country general profile. If no, specify which standards have been implemented in the eSignatures application? Depending on the signature type, this may include standards regarding certificates, signature formats, signature algorithms, token formats, other information security standards, etc.	
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	*When a signed message is received the signature is verified against the attached certificate and the validity of the certificate is checked with the CA directly*
What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP…)	*Either CRL, OCSP or encrypted OCSP as indicated in the certificate*
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	*All information is securely archived in the DTI's Document Management System*

Organisational aspects	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	*The DTI as the Government department responsible for the Oil & Gas industry in relation to its activities on the UK's continental shelf; the Oil & Gas companies in their dealings with this aspect of the DTI and external, approved CAs that issue the certificates*
Who are the relying parties[14]? Describe the context?	*For signed data provided by the Oil & Gas companies, the DTI is the relying party and vice versa*
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	*Approved commercial CAs or approved internal CA functions, where approval is by tScheme or an equivalent scheme*
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be	*Usually 2-year validity and certificates will be revoked where there is or suspected to be compromise of the private key (plus other reasons as detailed in the CP of the relevant*

[14] « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

suspended or revoked?	*CA)*

10.3.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	*Nationality is not an issue as certificates are issued to employees of the relevant Oil & Gas company on the basis of their role within that organisation*
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	*Country of origin of certificate is not relevant*

10.3.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	*Application used in all licences and consents issued in 2006 (between 1000 and 5000)*
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	*None*
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	*None since this is a niche solution and all participants are aware of the scheme*

10.3.5 Assessment

Assessment	
Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses). Take this opportunity to bring any fruitful information that was not addressed by previous questions.	*The use of eSignature have been implemented using standard document signing capabilities (e.g. Adobe Acrobat) and as a result have produced the strength of solution envisaged at the commencement of the project*