CABINET
OFFICE

Office of the *e-Envoy*
Leading the drive to get the UK online

*delivering*
UK online

# Security Architecture

e-Government Strategy

Version 2.0
September 2002

# Contents

# Executive summary

*General*

This security architecture has been developed as part of the government's commitment, in the Modernising Government white paper[1], to developing a corporate IT strategy for government. It has been prepared by the Office of the e-Envoy, part of the Cabinet Office, on behalf of the e-Champions.

The security architecture is an evolving document and will be re-issued from time to time in line with changes in security framework policy and guidelines, implementation experience for UKonline services and market developments.

This document is aimed at those procuring and providing e-Government services. This includes Central Government Departments, non-departmental public sector bodies, Local Authorities and other local government bodies charged with the provision of e-Government services. It also encompasses regulatory bodies responsible for the proper audit and control of public assets and information.

In addition it includes the suppliers and service providers who wish to offer services themselves, provide and operate such systems on behalf of government or provide equipment in support of e-Government services.

*Background*

The government is engaged in a programme (branded as UKonline) to modernise the way in which services are delivered to clients[2]. It is envisaged that clients will transact electronically with government through a variety of channels, such as PCs, iDTV, mobile telephones and kiosks via a variety of central government, local government and private sector portals.

The portals will use Internet-based technologies, to bring information together and a government gateway to provide a common interface to the government back-office systems operated by central and local government departments and agencies. A portal may offer the client facilities to personalise the way they view the site. The government gateway provides appropriate common security services, including client authentication, confidentiality and privacy.

Once a client has been authenticated, the government gateway forwards information between the client and appropriate government back-office systems. It co-ordinates transactions on government back-office systems on behalf of the client to support 'joined-up' government services. The government gateway also provides a secure messaging facility to allow government to communicate with the client.

Some government back-office systems will be legacy transaction processing systems, while others may be internet-based. The variety of implementation approaches for the government back-office system has been a strong driver for the adoption of the portal and government gateway architecture.

[1] *Modernising government white paper.*

[2] A client is a person, an organisation, a duly authorised representative of the person or organisation or a process seeking to carry out a transaction with government.

*Objective and scope*

Establishing confidence and trust by clients will be one of the key success factors for the provision of UKonline services. The security framework and related guidelines provide a general framework for achieving this confidence and trust.

This security architecture supports the development of security for the UKonline services by providing: illustrations and guidance on how the security framework and related documents would be applied for particular illustrative on-line business scenarios at various levels of trust with currently available technologies and processes.

The security architecture is applicable to those components and systems that implement UKonline services, the government gateway and interfaces with government back-office systems.

*Overarching concept of operations*

The illustrations and guidance are based around an overarching concept of operations for the security aspects of UKonline services. This concept of operations is particularly aimed at registration and authentication, including roles, intermediaries and delegate accounts. Of particular note are the following main processes:

> registration in which a client establishes the client's real-world or electronic identity and the right to the identity; registration typically leads to the issue of a credential.
>
> enrolment at the government gateway in which a client initially establishes an electronic identity with the government gateway and subsequently authenticates for this identity;
>
> enrolment in which a client's right to use a particular UKonline service is established.

*Current government interim approach*

The security architecture is driven by the current interim government policy outlined below:

> all clients dealing electronically with government by 2005 will have one or more digital certificates to enable transactions that require higher levels of registration and / or authentication;
>
> the highest authentication level will require clients to hold secure signing devices such as a digital certificate held within a smartcard;
>
> the government will make use of third party registration and credential provision services that are aligned with the *tScheme* initiative (*eg* those provided by the banking and retail sectors) and that clients use in other day-to-day business;
>
> the government does not intend to perform registration services on its own behalf or to specify standards for digital certificates or smartcards or otherwise distort the market place (this implies that a credential such as a digital certificate need not contain or point to any personal information obtained during registration releasable for government use).

The interim approach adopted for the security architecture in the light of the above policy is to:

a. accept third party credentials normally only as evidence of an electronic identity; this effectively means ignoring the level of registration required for issue of the credential;

b. require the client to enrol for specific services; enrolment includes the collection of information from the client necessary for the provision of the service, including, where necessary, an asserted real-world identity; this information can typically be checked against information held on the back end system corresponding to the client's asserted real-world identity.

The enrolment process helps confirm the asserted real-world identity of the client (or in the case of an anonymous or pseudonymous service that the client is the same). It is envisaged that for higher levels of authentication, trust would be further enhanced by sending a one-time password to the client to authorise first use of a service by means of out of band (*eg* post) communications.

The interim approach is driven by what might be currently achievable. The government envisages and is pursuing in the medium term a move to a position where appropriate identification information provided by clients for third party registration will be releasable to support access to e-Government services. In particular, this would permit, where required, the electronic identity represented by, say, a digital certificate within a smartcard to be linked to a real-world identity. This approach would thus support enrolment at the government gateway and reduce the need for a separate enrolment activity. Some service specific enrolment might still be required to collect additional personal information.

*Specific implementations*

Any specific implementation will need to take into account the actual business context and needs, the access channels to be used, available technology and legacy systems together with detailed security advice.

Moreover, due reference must also be made to relevant legislation. Thos includes the Human Rights Act, the Data Protection Act, the Electronic Communications Act, the Public Records Act and the Regulation of Investigatory Powers Act.

# 1. Introduction

## 1.1 Ownership and maintenance

This security architecture has been developed as part of the government's commitment, in the Modernising Government white paper[3], to developing a corporate IT strategy for government. It has been prepared by the Office of the e-Envoy, part of the Cabinet Office, on behalf of the e-Champions.

The security architecture is an evolving document and will be re-issued from time to time in line with changes in policy and implementation experience for UKonline services.

This version of the document is for issue by the Office of the e-Envoy. It should be noted that the security framework and the various security guidelines have been revised substantially. Annexes C, D, E, G reflect the current versions of these documents.

## 1.2 Terminology

A list of abbreviations is provided at annex A. The meaning ascribed to specific terms in the document is provided in the glossary at annex B, This glossary is the common glossary being used for the revised security framework and the various security guidelines.

## 1.3 Who should read this document?

This document is aimed at those procuring and providing e-Government services. This includes Central Government Departments, non-departmental public sector bodies, Local Authorities and other local government bodies charged with the provision of e-Government services. It also encompasses regulatory bodies responsible for the proper audit and control of public assets and information.

In addition it includes the suppliers and service providers who wish to offer services themselves, provide and operate such systems on behalf of government or provide equipment in support of e-Government services.

## 1.4 Background

The government is engaged in a programme (branded as UKonline) to modernise the way in which services are delivered to citizens, businesses and other organisations.

It is envisaged that a client[4] who wishes to transact electronically with government will be able to do so through a variety of channels, such as Personal Computers (PCs), interactive Digital Television

[3] *Modernising government white paper.*

(iDTV), mobile telephones and kiosks. All these channels will enable the client to access a variety of government and private sector portals (web sites) to perform transactions with government, be that searching for publicly available information, submitting an electronic form or receiving information of personal relevance. An overview of the proposed architecture is shown at Figure 1 below.

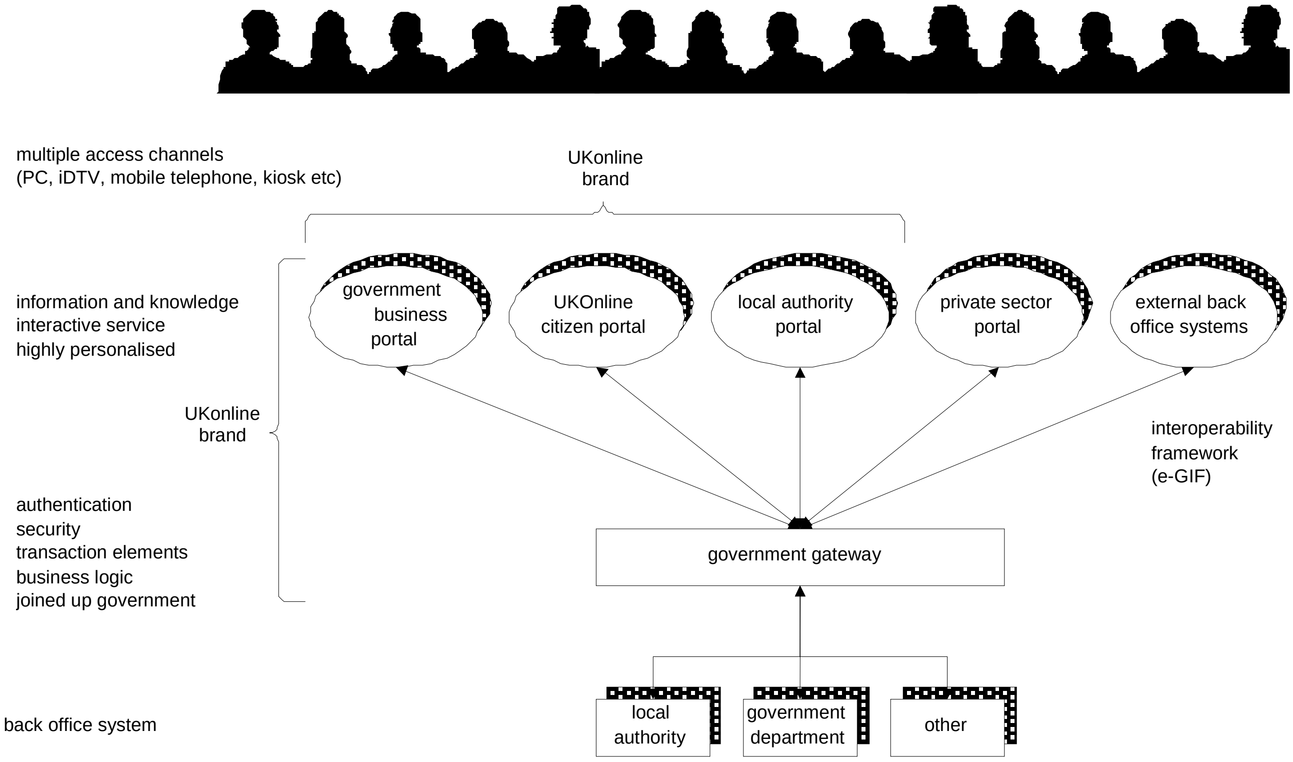


Figure 1: Portal and government gateway architecture

### 1.4.1 UKonline brand

The UKonline brand refers to the provision of government services by electronic means. The service provider could be, for example, one or more of a central government department, a government agency, a local authority or a private sector organisation acting on behalf of local or central government.

### 1.4.2 Portals

The UKonline citizen portal is the electronic interface between clients and the government. It will be accessed through Internet-based technologies, use websites to bring information together and a gateway to provide a common interface to the back-office systems operated by government departments and agencies. The UKonline citizen portal will also present publicly available information.

There may be other portals (*eg* local authority portal or a government business portal) together with private sector portals and external back-office systems. All of the government portals and the government gateway are within the UKonline brand.

A portal may offer the client facilities to personalise the way they view the site. This will allow the site designers to bring to the attention of the client new and changing content that the client has labelled interesting to them. This type of personalisation can be based around ‘life events’, such as I’m Having a Baby or I’m Moving House so that content (including advertising) and transactions relevant to these

[4] A client is a person, an organisation, a duly authorised representative of the person or organisation or a process seeking to carry out a transaction with government.

events could be displayed to the client. Such transactions may require processing by more than one government department.

### 1.4.3 Government gateway

The government gateway provides the bridge between the various portals and external back-office systems and the back-office systems operated by government departments, local authorities and private sector service providers. It provides appropriate common security services, including client authentication, confidentiality and privacy.

Once a client has been authenticated, the government gateway forwards information between the client and appropriate government back-office systems. It co-ordinates transactions on government back-office systems on behalf of the client to support 'joined-up' government services covering a number of government departments and agencies (*eg* the gateway would co-ordinate a change of address function).

The government gateway also provides a secure messaging facility to allow government to communicate with the client. This permits, for example, a government department to communicate with a client as part of the processing carried out.

### 1.4.4 Government back-office systems

Some government back-office systems will be legacy transaction processing systems, while others may be internet-based. The variety of implementation approaches for the government back-office system has been a strong driver for the adoption of the portal and government gateway architecture.

### 1.4.5 Security framework

Establishing confidence and trust by clients will be one of the key success factors for the provision of UKonline services. Clients will need to be confident that a service is secure and that their privacy is being maintained. The security framework[5] and related documents[6,7,8,9,10] are directed at achieving this confidence and trust. In particular, the:

a. UKonline services should be secure: any information that is passed to it by the client should be protected and controls should be provided that mitigate external threats such as attempted penetration by hackers, and misuse by authorised users;

b. UKonline services should be available: measures should be provided to prevent either the physical delivery of the service becoming unavailable or client's service data becoming corrupted;

c. UKonline services should be identifiable: when required, measures should be provided to ensure that the electronic identity of the government gateway and / or UKonline service is known securely to clients and that transactions are accountable to all parties;

[5] The latest version of *e-Government strategy framework policy and guidelines, security*. Available at http://www.e-envoy.gov.uk

[6] The latest version of *e-Government strategy framework policy and guidelines, registration and authentication*. Available at http://www.e-envoy.gov.uk

[7] The latest version of *e-Government strategy framework policy and guidelines, trust services*. Available at http://www.e-envoy.gov.uk

[8] The latest version of *e-Government strategy framework policy and guidelines, confidentiality*. Available at http://www.e-envoy.gov.uk

[9] The latest version of *e-Government strategy framework policy and guidelines, network defence services.* Available at http://www.e-envoy.gov.uk

[10] The latest version of *e-Government strategy framework policy and guidelines, business services*. Available at http://www.e-envoy.gov.uk

d. clients should be identifiable: when required, measures should be provided to ensure that the electronic identity[11] of a client is known securely to those with whom they are dealing and that transactions are accountable to all parties.

It is intended that all government bodies, and organisations providing electronic services on their behalf, will carry out security in a consistent manner when doing business electronically.

## 1.5 Objective of the security architecture

The security architecture builds on the security policy as defined in the security framework document[12] that sets out the security requirements expressed in the corporate government IT strategy.

The objective is to support the development of security for the UKonline services, the government gateway and related portals by providing illustrations and guidance on how the security framework and related documents would be applied for particular on-line business scenarios with currently available technologies and processes. This includes:

a. an overarching concept of operations for using UKonline services;

b. the proposed concept of operations for registration and authentication of clients at various levels of trust;

c. security issues that might arise from the UKonline concept;

d. initial guidance on how particular security functionality might be implemented;

e. those areas that require further work and the strategy for their resolution.

## 1.6 Scope

The security architecture specified in this document is applicable to those components and systems that implement UKonline services, the government gateway and interfaces with government back-office systems.

## 1.7 Organisations affected by this security architecture

The security architecture applies to all organisations that provide UKonline services by or on behalf of the government.

Central government departments and agencies must comply with the security architecture. In particular, when introducing a UKonline service, a central government department will:

a. adopt the overarching concept of operations for UKonline services and the outline security architecture;

[11] Depending on the particular transaction, an identity can be associated with a named individual, be anonymous or be pseudonymous.

[12] The latest version of *e-Government strategy framework policy and guidelines, security*. Available at http://www.e-envoy.gov.uk

b. adopt the concepts of operations for registration and authentication provided within the security architecture;

c. adopt the model of security functions within the architecture;

d. note the guidance and security issues identified within the architecture.

It is strongly recommended that other public sector bodies adopt the security architecture in respect of UKonline services that they conduct with businesses and the public or which are conducted on their behalf.

## 1.8 Relationship to other framework documents

The security architecture is to be read in conjunction with the security framework and related documents identified at section 1.4.5 above.

# 2. Security architecture

## 2.1 Introduction

This section sets out the outline security architecture for secure interactions between a client and the government gateway. The security architecture is established within the context of an overarching concept of operations. Some elements of the concept of operations are driven by current government policy as described below.

## 2.2 Overarching concept of operations

### *2.2.1 Introduction*

*Figure 2* overleaf provides a conceptual overarching concept of operations for a client accessing UKonline services utilising the government gateway. The concept of operations comprises the following processes that are described further below:

a. registration;

b. enrolment at the government gateway, where that is required;

c. enrolment for particular services;

d. authentication and service use;

e. service or government gateway authentication;

f. disenrolment on completion of need for a specific enrolled service;

g. disenrolment from the government gateway on completion of need for UKonline services.

From the user's view, a number of these may be combined, depending on portals and services used. For example, a request to enrol for a particular service could initiate registration and gateway enrolment.

The term client is used in this document to mean:

a. a person;

b. an organisation;

c. a duly authorised representative of the person or organisation acting as an agent;

d. a process

that is seeking to carry out a transaction with government.

The overarching concept of operations also addresses roles, intermediaries and delegate accounts.

The processes span the physical domain, a government gateway UKonline session or one or more service sessions, associated with specific on-line services available from a government back-office system utilising the government gateway.

These processes may not all be a government gateway responsibility (*eg* current policy is for the government gateway not to be responsible for registration for a digital certificate, that is required to access some services).

### 2.2.2 Current government policy and implications for the concept of operations

Certain elements of the concept of operations described in this document are driven by the following interim government policy:

> all clients dealing electronically with government by 2005 will have one or more digital certificates to enable transactions that require higher levels of registration and / or authentication;
>
> the highest authentication level will require clients to hold secure signing devices such as a digital certificate held within a smartcard;
>
> the government will make use of third party registration and credential provision services that are aligned with the *tScheme* initiative (*eg* those provided by the banking and retail sectors) and clients use in other day-to-day business;
>
> the government does not intend to perform registration services on its own behalf or to specify standards for digital certificates or smartcards or otherwise distort the market place (this implies that a credential such as a digital certificate need not contain or point to any personal information obtained during registration releasable for government use).

The interim approach adopted for the security architecture in the light of this interim policy is to:

a. accept third party credentials normally only as evidence of an electronic identity; this effectively means ignoring the level of registration required for issue of the credential;

b. require the client to enrol (see section 2.2.5) for specific services; enrolment includes the collection of information from the client necessary for the provision of the service, including, where necessary, an asserted real-world identity; this information can typically be checked against information held on the back end system corresponding to the client's asserted real-world identity.

The enrolment process helps confirm the asserted real-world identity of the client (or in the case of an anonymous or pseudonymous service that the client has the same anonymous or pseudonymous identity). It is envisaged that for higher levels of authentication, trust would be further enhanced by sending a one-time password to the client to authorise first use of a service by means of out of band (*eg* post) communications.

The interim approach is driven by what might be currently achievable. The government envisages and is pursuing in the medium term a move to a position where appropriate identification information provided by clients for third party registration will be releasable to support access to e-Government services. In particular, this would permit, where required, the electronic identity represented by, say, a digital certificate within a smartcard to be linked to a real-world identity. This approach would thus

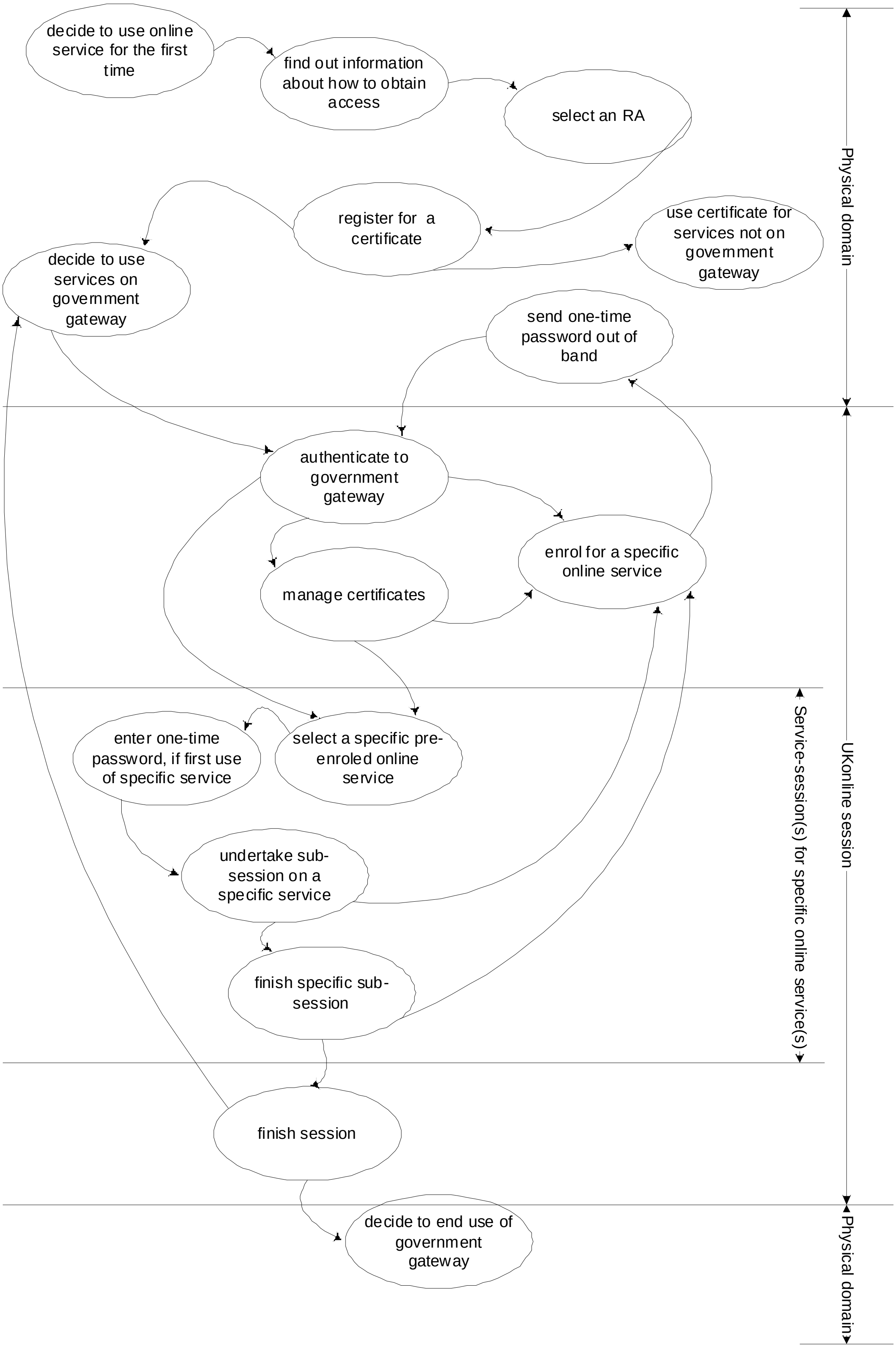

decide to use online service for the first time
find out information about how to obtain access
select an RA
register for a certificate
use certificate for services not on government gateway
decide to use services on government gateway
send one-time password out of band
authenticate to government gateway
enrol for a specific online service
manage certificates
enter one-time password, if first use of specific service
select a specific pre-enroled online service
undertake sub-session on a specific service
finish specific sub-session
finish session
decide to end use of government gateway
Physical domain
UKonline session
Service-session(s) for specific online service(s)
Physical domain

*Figure 2: The overarching concept of operations*

support enrolment at the government gateway and reduce the need for a separate enrolment activity. Some service specific enrolment might still be required to collect additional personal information.

### 2.2.3 Registration

A client first decides that he or she wishes to make use of an UKonline service and then determines the necessary steps to gain access to the service. For those UKonline services that need it, the client carries out any pre-requisite activities to establish the client's identity and the right to the identity. Registration typically leads to the issue of a credential[13] (*eg* a client identifier and password or a digital certificate). Registration can be associated with a real-world identity or can be anonymous or pseudonymous.

The client might acquire and use the credential to gain access to commercial on-line services. The client might use these services before deciding to use an UKonline service.

Examples of registration include:

a. obtaining a client identifier and password combination from a government department to use the UKonline services for that department (*eg* as is currently the case with the Inland Revenue);

b. obtaining a digital certificate for use of an on-line banking service that can also be used for access to UKonline services; this service could be accessed via, for example, a PC, a Wireless Access Protocol (WAP) phone or in the future a kiosk; in this example, the credential is bound to the client's real-world identity; this assumes that Government and the provider of the on-line banking service have reached an agreement on transfer of liabilities;

c. obtaining a digital certificate anonymously; this would be appropriate for anonymous access to information where the service provider needs to be sure that the same client is using the service each time (*eg* anonymous medical screening).

The registration process might require the client to provide common basic information (*eg* name, address, telephone number, e-mail address, National Insurance (NI) number *etc*). The use of such information is discussed in section 2.2.5.

The registration process typically occurs within the physical domain (*eg* face to face review of information presented to establish an identity) or within the IT domain (*eg* electronic presentation of documents *etc* required as part of a registration process for a digital certificate).

Any party with a need to trust a credential to associate an identity with a client is referred to as the Relying Party (RP).

### 2.2.4 Enrolment at the government gateway

After registration is completed and the appropriate credential issued, the client might decide at some stage to use an UKonline service. For those UKonline services that need it, the client first enrols with the government gateway in an initial on-line session by presenting an acceptable credential (*eg* entering a client identifier and password or by presenting a digital certificate / smartcard). The purpose of this is to establish the identity of the client with an appropriate degree of trust. Enrolment at the government gateway can be associated with a real-world identity or can be anonymous or pseudonymous.

The government gateway will check the validity of the credential and set up a directory entry corresponding to the credential and containing information specific to the client (section 2.5).

[13] Depending on the particular transaction, the credential can be associated with a named individual, be anonymous or be pseudonymous.

To address privacy and confidentiality concerns, it is envisaged that the directory will not hold any information on clients other than that needed to map between the credential and the government back-office services.

After successful enrolment at the government gateway, the client may enrol for one or more UKonline services (see section 2.2.5).

On a subsequent visit, the client presents the credential and correct client verification information, the government gateway checks the validity of the credential and, if the results are positive, the client is authenticated. This includes checking that the directory entry is present.

The period between a client successfully registering or authenticating with the government gateway and ending the use of the service for a specific occasion is referred to as an UKonline session.

Different authentication levels are required for credentials, depending on the specific service required. A credential issued at a particular authentication level can also be used for registration and authentication at each lower authentication level.

### 2.2.5 Enrolment for particular services

After successful enrolment at the government gateway, the client may enrol for one or more specific UKonline services. Some services will require the client to establish a real-world identity and others will be anonymous or pseudonymous. Moreover, particular services (*eg* submission of a personal tax form) may have pre-existing information concerning the client held on the government back-office systems, while others (*eg* on-line learning) may not.

It is envisaged that the client will be offered a tailored list of UKonline services for enrolment, based on the type of credential offered and on trust established by the current successful enrolments. For example, a digital certificate / smartcard that was obtained after a face-to-face interview and that included a strongly bound real-world identity would potentially be offered a wider range of services than an anonymous digital certificate / smartcard that had no previous enrolments.

Part of the enrolment process would involve the government gateway collecting information from the client that is essential for the operation of the specific on-line service. It is envisaged that only essential information that is not already held would be collected. The information collected is stored in the directory. This would include sufficient information to identify the records corresponding to a client, if any, held on a government back-office system (*eg* name, NI number, tax reference number *etc* for an Inland Revenue service).

This information helps confirm that the real-world identity of the client (or in the case of an anonymous or pseudonymous service that the client is the same) by comparing the collected information with information already held by the government back-office system for the asserted identity. For services needing a real-world identity, a particular benefit of this approach is that as the client successfully enrols in more services that require validation against information held on government back-office systems, the level of trust in the identity is enhanced. Similarly, for services supporting anonymous or pseudonymous identities, as the client enrols in more services, the level of trust in the client being the same as last time is enhanced.

It is envisaged that for higher levels of authentication, trust would be further enhanced by sending a one-time password to the client to authorise first use of a service by means of out of band (*eg* post) communications. This would reduce the possibility of spoofing a real-world identity.

Once the identity is established, this information allows the government gateway to map uniquely between the client's credential and the corresponding information held on the government back-office system supporting the service requested by the client.

Once a client has enrolled for a specific service, the client may access that service. Subsequent access to the service will require authentication to the gateway. The period of access to a specific on-line service is referred to as an UKonline service session.

It is likely that there will be inconsistencies between government back-office records and the client-provided information (*eg* a particular government back-office system may still have a previous address for the client). There might even be no corresponding information held by a government back-office system (*eg* the individual might not yet have a NI number). The outcome for enrolment will depend upon the detailed registration and enrolment policy for each government back-office service. Some enrolment requests may require referring to an adjudicator for a final decision. The government back-office system will need to establish a process to allow the client to resolve such issues in conjunction with the government gateway (*eg* using a helpdesk).

If enrolment is refused, the government gateway will need to consider what should be done about revoking any existing enrolments and/or access to UKonline. Again, the policy for this needs to be established in the detailed registration and enrolment policies.

### 2.2.6 Authentication and service use

The government gateway is a hub linking portals to government back-office systems. Amongst other things, the gateway provides authentication services. The linkage between a portal and a government back-office systems may be asynchronous, or synchronous. If it is asynchronous, the government gateway forwards information for a complete transaction to the government back-office system (and may provide secure messaging facilities for subsequent acknowledgement). If the linkage is synchronous, the client is effectively interacting with the government back-office system in real time. It is envisaged that the government gateway will become, in due course, the main link between clients and government back-office systems for government electronic service delivery.

The service application may need to engage in a further dialogue with the client to elicit information needed to undertake the transaction.

When the service application has completed the dialogue with the requesting client, it may undertake basic validation of the elicited information, and undertake additional interaction with the client if errors with the information are found. Once validation is successful, the service application will transmit the validated information to government back-office system(s) (if working asynchronously), and confirm to the requester that the transaction has been submitted.

For asynchronous transactions, the government back-office system(s) is able to use secure messaging to reply to the requesting client on the outcome of the transaction. For synchronous transactions, this information should be directly available to the client.

The client might choose to have simultaneous service sessions (*eg* a client could require information concerning a state pension to help complete an on-line tax return). The client might also choose to enrol for additional on-line services.

Normally, the client would terminate each UKonline service session and finally terminate the UKonline session.

On subsequent UKonline sessions, the client once authenticated for UKonline would be able to select and be authorised for on-line services for which he or she had already enrolled.

Facilities must be provided to allow a client to opt out from a service, and therefore, have appropriate information deleted from the directory. Again, such facilities must be subject to authentication.

### 2.2.7 Service or government gateway authentication

For some e-Government business processes, it might be necessary and appropriate for the service and/or government gateway to establish its identity to give assurance to the client that he or she is really accessing the service or government gateway. It is the government's vision that this will be supported by use of a digital certificate, issued to the service or gateway after a suitable registration process.

### 2.2.8 Disenrolment on completion of need for a specific enrolled service

At some point, the client might decide that a specific UKonline service was no longer required. The client once authenticated would request that the specific enrolment should be removed. All relevant information would be archived and appropriate accounting entries made. The government gateway would also inform the relevant government back-office system, if appropriate.

### 2.2.9 Disenrolment initiated by the client on completion of need for UKonline services

At some point, the client might decide that no further UKonline services were either required, or would otherwise cease to use UKonline services. In either case, subject to appropriate authentication, the client enrolments and right to use the government gateway would be deactivated, all relevant information archived and appropriate accounting entries made. The government gateway would also inform relevant government back-office systems, if appropriate.

### 2.2.10 Deregistration initiated by the government gateway

If a credential is revoked or if an enrolment for a particular service is suspected of being fraudulent, there needs to be a mechanism to deregister the client on a temporary basis to prevent use of e-Government services by the client until the revocation or enrolment concerns have been resolved.

## 2.3 Roles, intermediaries and delegate accounts

*Multiple roles*

If a client can interact with government in one of several roles (for example, as an employer and an employee), the system must determine which role is appropriate for a given transaction. This may be achieved by issuing distinct credentials for each role, or by allowing the client to choose which role is appropriate at transaction time. In either case, it is envisaged that appropriate directory entries will be required to govern which transactions a client may undertake.

*Intermediaries*

Intermediaries may be businesses or individuals that need to undertake transactions with government on behalf of others. Examples are payroll bureaux, accountants and individuals with a power of attorney. Intermediaries will be expected to obtain credentials as businesses or individuals, but in addition, the RP will need to obtain consent from a client for the intermediary to act on his behalf. Mechanisms must be provided to assert, check and revoke this authority to act.

Mechanisms are provided on the government gateway to maintain the mapping between third parties and their intermediaries. In particular, the mapping may only be maintained if both the third party and the intermediary agree, and the mapping must be removed if either the third party or the intermediary requests it. The government gateway must manipulate this mapping based on transactions with government back-office systems.

Note that intermediaries may be permitted to act on behalf of clients who have not registered for any electronic service.

It should also be noted that third parties may undertake some transactions themselves (and may indeed use delegate accounts to do this), but use an intermediary (who may also use delegate accounts) for other services. The directory mechanism in the government gateway must be sufficiently flexible to permit such arrangements, while maintaining appropriate security and authentication mechanisms.

*Delegate accounts*

Delegate accounts are client accounts created by trusted clients that can be enabled to undertake various services. They will typically be needed by large companies that employ many different people to undertake government transactions. It could be impractical for identity issuers to track the employees within a large company, and a single shared credential would need to be re-issued every time an employee left the company.

The solution proposed is for particular trusted clients to be permitted to manage their own delegate accounts, creating, manipulating and deleting entries in the government gateway as necessary. Clearly, the extent of this manipulation must be closely controlled. In particular, delegate accounts should not be able to enrol for, or opt out of, services. However, they should be able to create further delegate accounts. Government reserves the right for independent third party audit of this process.

## 2.4 Registration and enrolment policy statement

It is envisaged that there would be a registration and enrolment policy statement for the government gateway covering:

a. precisely which clients are entitled to register in accordance with guidelines for inclusivity;

b. what is the appropriate type of registration for each UKonline service;

c. what information needs to be collected from a client during enrolment at the government gateway and enrolment for each UKonline service;

d. precisely what credentials (*eg* smartcards / digital certificates) are acceptable to the government gateway, what UKonline services would be available for each and the means for checking the validity of each credential;

e. the appeals process if a client is rejected during enrolment at the government gateway;

f. the relationship between a credential provider and the government gateway, including the UKonline services that could be used by a credential holder and the apportionment of liabilities (*eg* for fraud).

Particular issues that might need to be considered in the registration and enrolment policy include whether:

a. the client needs to be a citizen;

b. the client needs to be above the age of majority for a particular service (*eg* checking name and address information against the electoral register could be a part of the registration process);

c. the client needs to have a fixed address to register (*eg* posting a one-time password to the client's registered address might be a part of establishing the client's identity for registration purposes or for sending a certificate to on successful completion of an online learning course).

## 2.5 Security architecture

Within the context of the overarching concept of operations, *Figure 3* below provides an overview of the security architecture for the government gateway.

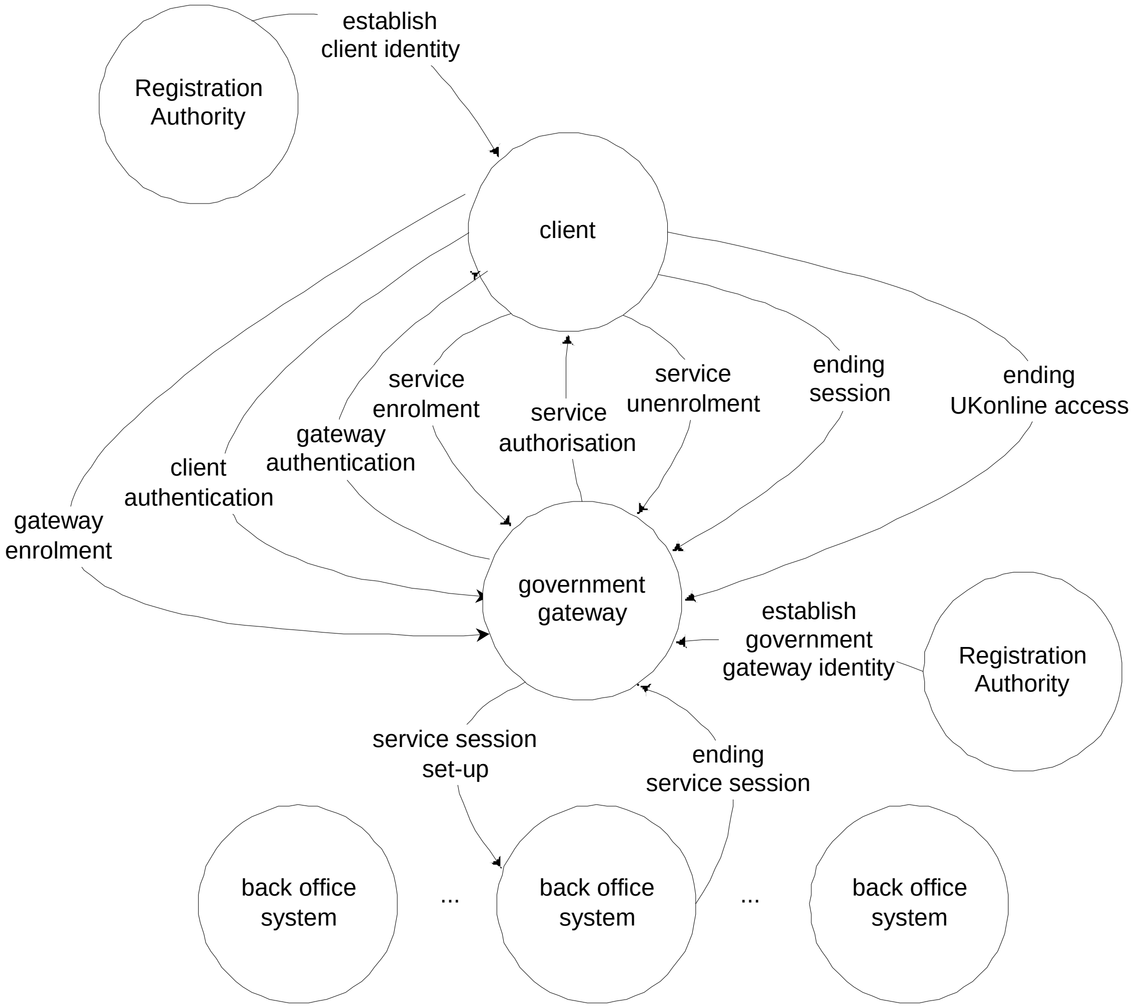


*Figure 3: Overview of the security architecture for the government gateway*

The Registration Authorities are included for completeness. These are required as part of the process of identifying an individual for issuing a digital certificate (see section 6.2.1).

In this model, the government gateway is the focus for interaction with the client. The government gateway holds an information store (referred to as a directory entry) containing information on each client. This directory entry is used to:

a. support confirmation of the identity of a client requesting authentication;

b. identify those services for which the client is enrolled;

c. hold the necessary information to enable a specific UKonline service to select and present the correct information for the client from the relevant government back-office system(s);

d. hold personalisation information for the client.

A key architectural issue is what personal information should be stored and/or retained for each client by the government gateway and what privacy and confidentiality protection should be provided. The directory information held on the government gateway is sensitive, because of both the privacy and confidentiality of the client to which it refers, and because this information provides the linkage between the requesting client and identities recognised by government back-office systems. The aggregation of primary key information represents a private association of data.

The policy is that information provided to each government back-office system from the directory will be limited to that necessary for that system to carry out the requested service.

There is a trade-off between privacy and confidentiality, and convenience. For example, personal information (*eg* name, address, tax reference and NI number *etc*) if stored on the government gateway could be used to ease the task of enrolling for further UKonline services. Conversely, the client might feel that this accumulation of personal information was not appropriate. One approach is for the client to use multiple credentials with one credential being used for a specific group of UKonline services.

Mechanisms must be in place to protect this information on the government gateway. In addition, the client must not have an unconstrained ability to alter it. Any access to this information by a client, for example, to satisfy the Data Protection Act (DPA), must be subject to authentication to at least a level as high as the highest level at which that client may undertake transactions.

The security architecture represents the overarching concept of operations in terms of the following logical security functions:

a. registration:

   i. establishing the identity[14] of the client;

   ii. establishing the identity of the government gateway;

b. enrolment at the government gateway:

   i. registering a client to use the government gateway;

   ii. authenticating the client to use the government gateway;

c. government gateway authentication:

   i. authenticating the government gateway to the client;

d. enrolment:

   i. enrolling for an UKonline service;

   ii. authorising a client to use an UKonline service;

[14] Depending on the particular transaction, an identity can be associated with a named individual, be anonymous or be pseudonymous.

e. service use:

   i. government gateway initiating a service session for a client with a government back-office system;

   ii. ending a service session;

   iii. disenrolment of a client from an UKonline service;

   iv. ending an UKonline session;

f. completion of the need for service use:

   i. deregistration initiated by a client;

   ii. deregistration initiated by the government gateway.

The concept of operations and the implementation approach for these logical functions will differ according to the underlying business need and associated security requirements. In some cases some of the functions might be redundant (*eg* there is no need to identify the client when anonymous or pseudonymous access is required.

These logical functions are examined in terms of both the concept of operations and implementation approach for the government gateway by exploring the scenarios defined in the next section.

### 2.5.1 Supporting functions

The logical security functions are supported by the security elements summarised at Figure 4 overleaf. The Certification Authorities (CAs) are included for completeness. These are required as part of the process of confirming the identity of a client using a digital certificate (see section 6.2.1).

The supporting security primitives comprise:

a. government gateway forwards information to a government back-office system;

b. government back-office system sends information to government gateway;

c. client sends information to government gateway;

d. government gateway sends information to client;

e. government gateway saves information concerning a client;

f. government gateway retrieves information concerning a client;

g. government gateway requests information concerning the identity of a client from a credential issuer;

h. CA provides information to the government gateway concerning a client (*eg* client’s revocation status, information collected during registration that a client is willing to release);

i. client requests information concerning the identity of a government gateway from a CA;

j. CA provides information to the client (*eg* government gateway’s revocation status);

k. government gateway makes an accounting entry concerning particular accountable events (*eg* successful and failed client authentications *etc*);

l. government gateway retrieves accounting entries for subsequent analysis.

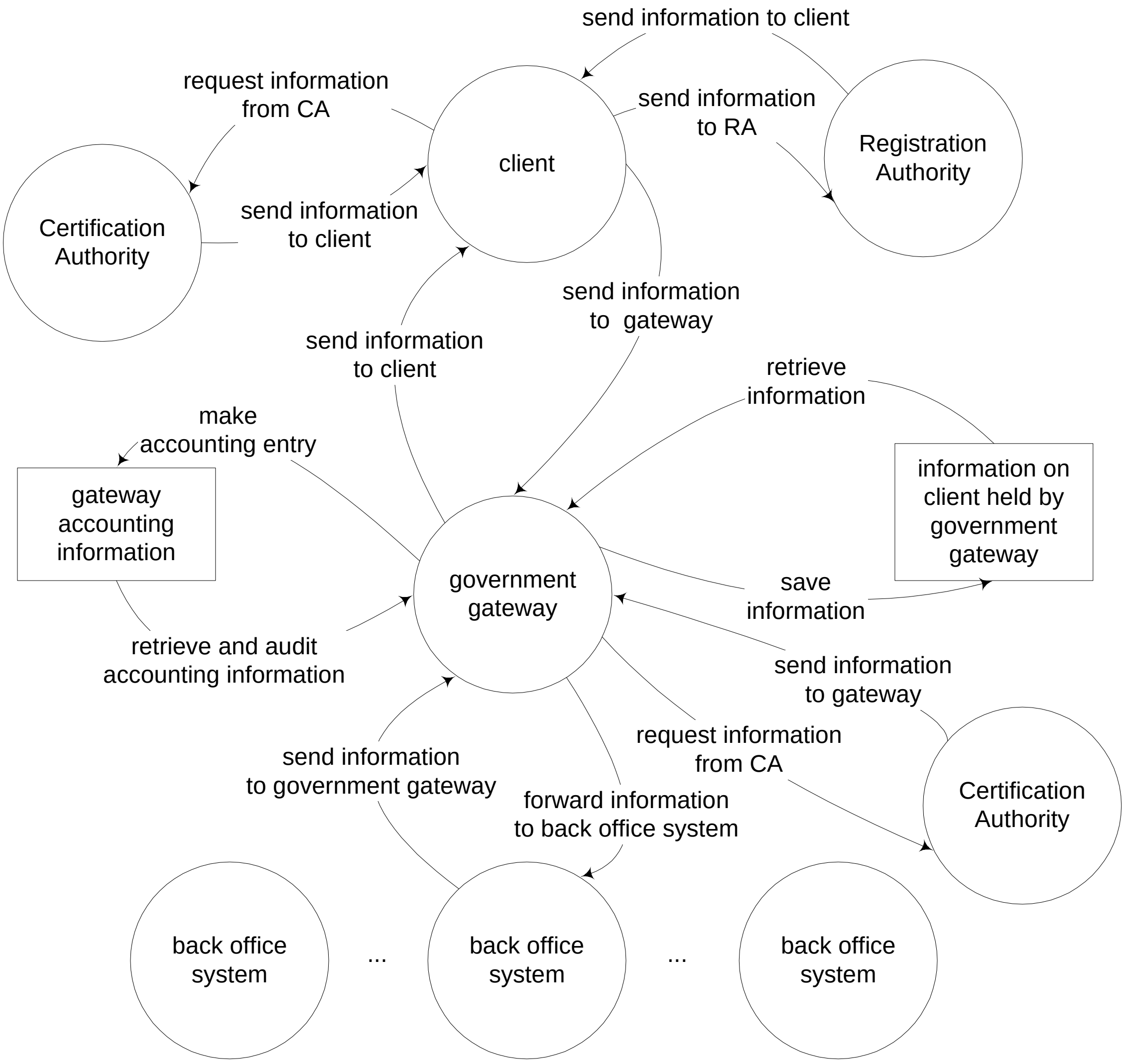

send information to client
request information from CA
client
send information to RA
Registration Authority
Certification Authority
send information to client
send information to gateway
send information to client
retrieve information
make accounting entry
gateway accounting information
information on client held by government gateway
government gateway
save information
retrieve and audit accounting information
send information to gateway
request information from CA
Certification Authority
send information to government gateway
forward information to back office system
back office system
...
back office system
...
back office system

Figure 4: Overview of the supporting functions for the security architecture for the government gateway

In each case, the security primitive will need to support the required confidentiality, integrity and non-repudiation characteristics.

Figure 4 also includes the following additional security primitives concerning communication between a client and a Registration Authority (RA):

a. client sends information to RA;

b. RA sends information to client.

No assumptions are made as to the RA and the CA being part of the same organisation.

## 2.6 Assurance

The e-Government assurance[15] process is built upon the principle of demonstrating compliance with the security policy framework. The approach comprises:

a. producing a security policy, preferably compliant with part I and part II of BS7799;

b. analysing the threats and vulnerabilities to the system and producing a risk assessment;

c. addressing the risks by applying appropriately assured countermeasures;

d. checking that the system configuration is compliant with the security policy;

e. assessing the residual risk and repeating steps c and d above until the residual risk is acceptable;

f. periodically reviewing the assurance status of the countermeasures and making appropriate changes.

[15] The latest version of *e-Government strategy framework policy and guidelines, assurance*. Available at http://www.e-envoy.gov.uk

# 3. Scenarios

## 3.1 Introduction

This section sets out representative scenarios for use of government gateway systems. The scenarios comprise:

a. S0: a client accessing publicly available information;

b. S1: a client interacting with an online learning system;

c. S2: a client interacting with the Inland Revenue;

d. S3: informing a client of the results of medical screening.

The security architecture assesses the level of protective measures required for each of the security objectives, OS1 to OS13[16], set out in the security framework document[17] with particular emphasis on the implementation of security objectives OS1 to OS9. The implementation of the remaining security objectives, OS10 to OS13, is outside the scope of this document:

## 3.2 Status of the scenarios

The scenarios are for illustration only with the intention of demonstrating the approach to the security architecture, the issues that might arise and the way to address them.

A specific implementation would need to take into account the actual business context, the detailed business needs, the access channels to be used, available technology and legacy systems and detailed security advice. In particular, any statement of the level of security requirements in this document is not to be taken as an agreement that these would be acceptable in practice.

Moreover, due reference must also be made to legislation that regulates data storage, electronic communications and law enforcement (*eg* the Human Rights Act, the DPA, the Electronic Communications Bill, the Public Records Act and the Regulation of Investigatory Powers Act). The interpretation of these implied requirements is outside the scope of this security architecture.

[16] The security objectives are: OS1: Effective user identification and authentication; OS2: Effective user registration; OS3: Effective access control; OS4: Effective user access management; OS5: Non repudiation; OS6: Evidence of receipt; OS7: Trusted commitment service; OS8: Privacy and confidentiality; OS9: Integrity; OS10: Service availability; OS11: Information availability; OS12: Service protection; OS13: Effective audit and accounting.

[17] The latest version of *e-Government strategy framework policy and guidelines, security*. Available at http://www.e-envoy.gov.uk

## 3.3 S0: accessing publicly available information

In this scenario, the client requests publicly available information from a government department by e-mail. The government department uses the government gateway secure messaging facility either to:

a. send the requested information to the client by return;

b. or, send a notification to the client that the information will be sent later and subsequently send it;

c. or, send a notification to the client that the information is available on a standard or specially constructed web page.

The client might be accessing the information for him- or herself or be informally acting on behalf of another citizen or organisation. (*eg* a professional advisor acting on behalf of a citizen, a relative acting on behalf of an individual or an employee acting on behalf of a company). The client might not be a UK citizen or organisation.

## 3.4 S1: interacting with an online learning system

In this scenario, the client selects, establishes, pays for and uses an online learning account with the objective of undertaking one or more courses. The application presents the client with learning materials together with assignments and tests for online completion and submission. Some assignments and tests might involve self-assessment, while others might be marked. The client's assignment and test marks are recorded. Successful completion of specific courses might lead to the issue of a recognised certificate. In this case, there needs to be an identified real-world identity.

The client would normally be acting on his or her own behalf. Use of the client's account by any other individual might be considered fraudulent. It is assumed that fraudulently obtaining the recognised certificate would only lead to minor financial loss by a third party (*eg* an employer).

## 3.5 S2: interacting with the Inland Revenue

In this scenario, the client wishes to interact with the Inland Revenue to undertake one or more of the following:

a. fill-out and submit a personal tax return on-line;

b. receive an assessment of personal tax liability on-line;

c. receive an electronic payment for overpaid tax to the client's account together with an electronic notification, using the government gateway secure messaging facility;

d. pay an income tax liability on-line using a credit or debit card.

The client might be acting on his or her own behalf or be authorised to act on behalf of another citizen or organisation (*eg* a professional advisor acting on behalf of a citizen, a relative acting under power of attorney or an employee acting on behalf of a company).

## 3.6 S3: informing a client of the results of medical screening

In this scenario, a citizen has undergone medical screening. The results of the screening would be sent to the citizen, for example, by the government gateway secure messaging facility. Under certain circumstances the citizen might choose to be anonymous or to use a pseudonym. However, it is essential that the results of the screening are sent to the same individual who underwent the screening.

The results could be either:

a. screening negative - no further action required;

b. screening positive - further action required with, for example, the citizen being offered a follow-up appointment.

The recipient of the electronic communication might be the citizen acting on his or her own behalf or be acting informally (*eg* a parent acting on behalf of a child) or formally (*eg* a friend or relative acting under a power of attorney) on behalf of another citizen.

## 3.7 Security requirements by scenario

Table 1 overleaf summarises for each scenario the assessed levels for the various security services for enrolment at the government gateway and for services provided by the portal and the government gateway. The detailed assessment is provided at the annexes shown in the table. The detailed assessment is provided at the annexes shown in the table.

| Security requirements by services | Scenario | | | | Security objectives covered | Domain or scope / comment |
|---|---|---|---|---|---|---|
| | S0 | S1 | S2 | S3 | | |
| | Annex C | Annex D | Annex E | Annex G | | |
| Registration[18] | Level 0 | Level 1/0[19] | Level 2 | Level 3/0 | OS2 | Clients seeking to access e-Government services, where there is a need for trust in the identity |
| Authentication | Level 0 | Level 1 | Level 2 | Level 3 | OS1, OS3, OS4 | |
| Trust[20] | Level 0 | Level 1 | Level 2 | Level 3 | OS5, OS6, OS7, OS9 | Support for clients and government entering into commitments for e-government services |
| Confidentiality[21] | Level 0 | Level 1 | Level 2 | Level 2 | OS8 | Information stored within systems providing e-Government services, in transit within and between such systems and clients |
| Network defence[22] | Level 1 | Level 1 | Level 2 | Level 3 | OS12 | Means of countering electronic threats associated with connecting business domains or IT resources |
| Business[23] | Level 1 | Level 1 | Level 2 | Level 3 | OS10, OS11, OS13 | Means of ensuring that the required level of business service is provided |

Table 1: Summary of security service levels by scenario

[18] The latest version of *e-Government strategy framework policy and guidelines, registration and authentication*. Available at http://www.e-envoy.gov.uk

[19] Depending on whether anonymity is required.

[20] The latest version of *e-Government strategy framework policy and guidelines, trust services*. Available at http://www.e-envoy.gov.uk

[21] The latest version of *e-Government strategy framework policy and guidelines, confidentiality*. Available at http://www.e-envoy.gov.uk

[22] The latest version of *e-Government strategy framework policy and guidelines, network defence services*. Available at http://www.e-envoy.gov.uk

[23] The latest version of *e-Government strategy framework policy and guidelines, business services*. Available at http://www.e-envoy.gov.uk

# 4. S0: accessing publicly available information

## 4.1 Introduction

This section sets out the concept of operations and implementation approach for scenario S0: accessing publicly available information. The security requirements for this scenario are set out at annex C.

These security requirements essentially conform to normal use of the Internet via the selected access channel (*eg* PC, mobile phone, kiosk).

## 4.2 Concept of operations

No additional concept of operations over and above that of the normal use of the Internet via the selected access channel is required.

In particular, there is no need for the client to establish formally his or her identity or for the government gateway to establish formally its identity. Clients can be anonymous or pseudonymous and could freely act on the behalf of other individuals or organisations. In particular, no specific controls need be established for multiple roles, intermediaries or delegate accounts.

There is no presumption as to whether the client is above the age of majority.

## 4.3 Implementation approach

The implementation approach here is to use standard Internet technology and architectures appropriate for each of the access channels.

Implementation needs to be to good commercial standards. Particular attention needs to be given to the policies, processes and practice for establishing, maintaining and using:

a. configuration management;

b. a virus checking regime for the publicly available information and for incoming information requests;

c. an information management policy for publicly available information;

d. a training regime for staff operating the government gateway or government back-office information service;

e. appropriate responses to any malicious or damaging activities that occur;

f. failure impact analysis for all domain connections;

g. backups of the publicly available information so that it can be restored as and when necessary.

# 5. S1: interacting with an online learning system

## 5.1 Introduction

This section sets out the concept of operations and implementation approach for scenario S1: interacting with an online learning system. The security requirements for this scenario are set out at annex D.

The scenario requires that authentication services at level 1 be used. The requirement at level 1 is for the presentation of a credential supported by additional private information. For this scenario, this is taken to be a client identifier supported by a secret password. The system will then authorise a client based on the validity of this credential/private information combination.

Registration for this scenario could be at level 0 or level 1. If level 1 registration is appropriate, the client could register either face-to-face or online by providing a personal statement together with appropriate documentary evidence[24]. If level 0 registration is appropriate, the client would register on-line for the client identifier and associated password. These would be available to the client immediately on registration. There would be no need for the client to provide any supporting evidence. For simplicity, the concept of operations presented below assumes level 0 registration carried out by the government gateway.

The client identifier might be the individual’s name or an alphanumeric string. The registration process might also be used to collect, for example, the client’s name, depending on whether a real-world identity is required or whether it is sufficient to ensure that the same individual is using the online learning account each time.

The client identifier and password remains active unless revocation is requested by the client or by the government gateway. Passwords do not expire and the client can change the password.

A client may choose to have a number of different client identifiers and use them to enrol for different subsets of available UKonline services. A client may also have different client identifiers to undertake separate roles (*eg* for professional and personal use). These separate client identifiers would not be associated with each other unless there was a specific legal need.

For the purposes of this scenario, it is assumed that the use of a known and trusted e-Government web site address provides sufficient trust in the identification of the site.

[24] The latest version of *e-Government strategy framework policy and guidelines, registration and authentication.* Available at http://www.e-envoy.gov.uk

## 5.2 Concept of operations

### 5.2.1 Registration

*Figure 5* overleaf provides the concept of operation for registration for scenario S1.

The client selects the registration option on the government gateway web page. The client then provides initial registration information to the gateway. This might include the client’s name, address, telephone number and e-mail address. The gateway might also request necessary further information (*eg* date of birth) to support the identity of the client, if required.

The gateway would carry out rudimentary checks on the information provided (*eg* check against the electoral register) or crosscheck the provided information against records held on the government back-office computer. If the checks are positive, the gateway will generate and issue a client identifier and password to the client using the government gateway secure messaging facility.

If the checks were negative, the government gateway would ask the client to confirm information already entered and possibly enter further information, depending on the detailed registration and enrolment policy. Finally, if the checks were still negative, the government gateway could refuse registration. The concept of operations allows the client to appeal against this decision. Again, the detailed registration and enrolment policy would need to be established.

The client might wish to change his or her password, if the original password had been forgotten. After appropriate checks on the client’s identity, the government gateway would generate and issue a new password to the client using the government gateway secure messaging facility.

The concept of operations also provides for revocation of the client identifier and password. This would be used, for example, if the client decided that access to the government gateway was no longer required, if it subsequently became known that the client’s identity was incorrect or if the client informs the gateway that the client identifier and / or password have been compromised or lost. In the latter case, after appropriate checks on the client’s identity, the government gateway would generate and issue a new client identifier and password to the client using the government gateway secure messaging facility Again, the detailed registration and enrolment policy would need to be established.

In the event of a revocation, the government gateway would send a confirmation of the revocation to the client using the government gateway secure messaging facility. This would help ensure the validity of the revocation request.

The overall registration management function is not shown. This would measure and monitor performance information and initiate appropriate management actions to ensure that management objectives and client expectations are managed and met.

It is assessed that a help desk should be established to support clients undertaking registration. This could be supported by e-mail and / or telephone. The help desk would also be used to resolve authentication, enrolment and UKonline service issues.

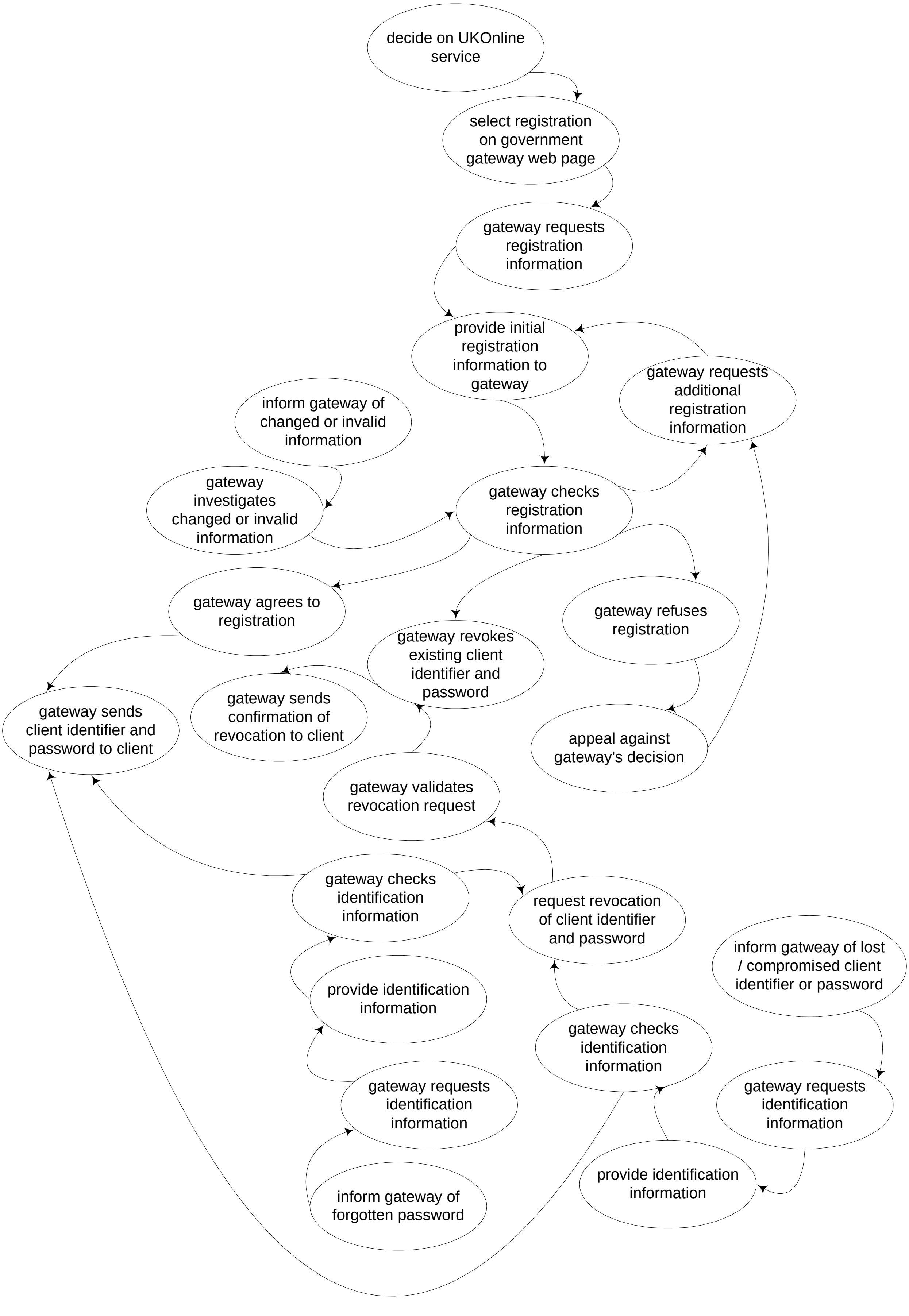

decide on UKOnline service
select registration on government gateway web page
gateway requests registration information
provide initial registration information to gateway
gateway requests additional registration information
inform gateway of changed or invalid information
gateway investigates changed or invalid information
gateway checks registration information
gateway agrees to registration
gateway revokes existing client identifier and password
gateway refuses registration
gateway sends client identifier and password to client
gateway sends confirmation of revocation to client
appeal against gateway's decision
gateway validates revocation request
gateway checks identification information
request revocation of client identifier and password
inform gatweay of lost / compromised client identifier or password
provide identification information
gateway checks identification information
gateway requests identification information
gateway requests identification information
provide identification information
inform gateway of forgotten password

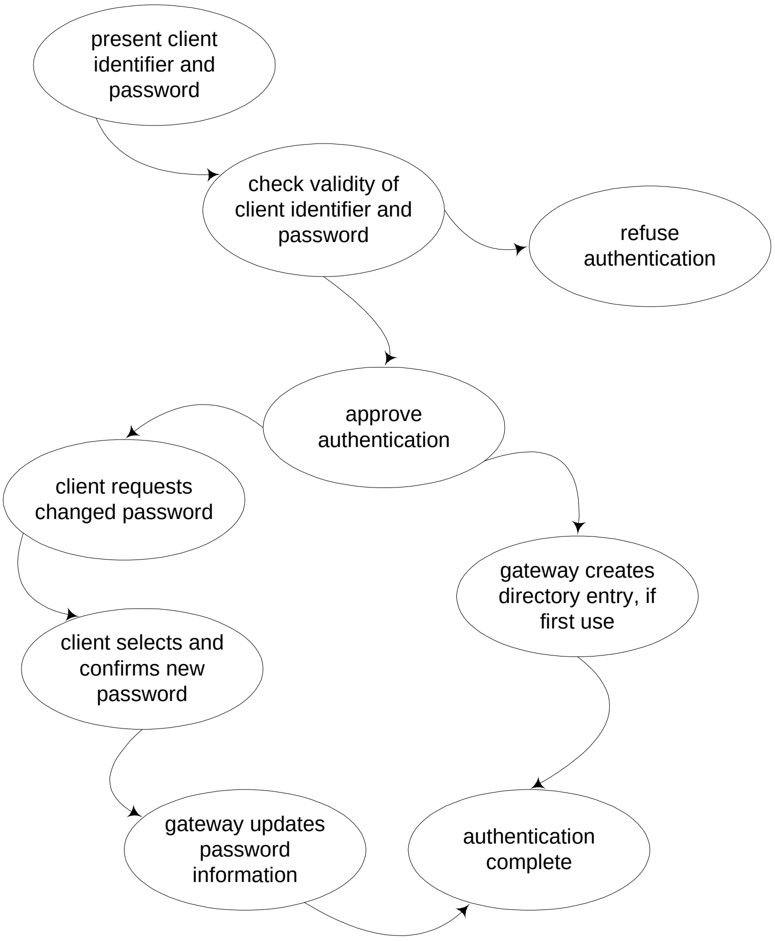
*Figure 5: Scenario S1: the concept of operations for registration*

### 5.2.2 Enrolment at the government gateway

*Figure 6* provides the concept of operation for enrolment at the government gateway for scenario S1.

The client presents the client identifier and password and the government gateway checks their validity. This includes checking whether the client identifier and password have been revoked as they have been compromised or lost. If the checks are positive, the government gateway authenticates the client for access on this occasion. If it is the first use of the client identifier, the government gateway creates the directory entry.

Once authenticated, the client can also request a password change. Once the client has confirmed the new password, the government gateway updates the client password information.



present client identifier and password
check validity of client identifier and password
refuse authentication
approve authentication
client requests changed password
gateway creates directory entry, if first use
client selects and confirms new password
gateway updates password information
authentication complete

*Figure 6: Scenario S1: the concept of operations for enrolment at the government gateway*

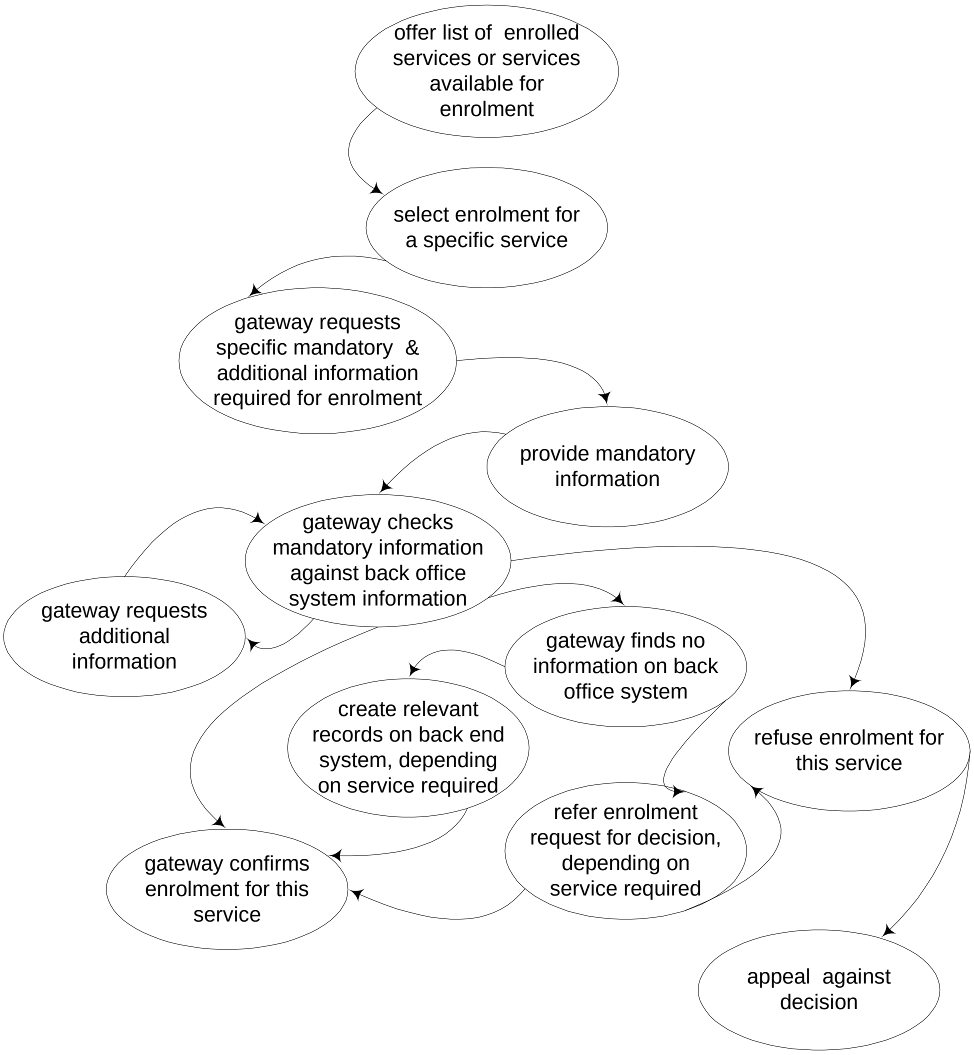
### 5.2.3 Enrolment

*Figure 7* overleaf provides the concept of operations for enrolment for scenario S1. It is assumed that for UKonline services at this level, the client would be allowed immediate access on enrolment.

Initially, the government gateway presents the client with a set of currently enrolled services and services that the client could enrol for at that level of authentication.

Depending on the type of service selected, there may be existing information regarding the client held on a government back-office system. In the case of enrolment for an on-line learning service, this is assumed not to be the case.

If the client selects enrolment in a new service, the government gateway will request any necessary additional information (*eg* for this scenario, this might be the client's name, address, educational attainment, credit card number *etc*). Once the client has entered this information, the government gateway will check it as far as possible and, if appropriate, will search the government back-office records for a match with the provided information. If the check was positive, the government gateway would allow immediate access to the service. If the check was negative, the government gateway would request creation of appropriate government back-office records, depending on the service selected for enrolment. This would apply to the case of online learning. Alternatively, enrolment would be refused.



offer list of enrolled services or services available for enrolment
select enrolment for a specific service
gateway requests specific mandatory & additional information required for enrolment
provide mandatory information
gateway checks mandatory information against back office system information
gateway requests additional information
gateway finds no information on back office system
create relevant records on back end system, depending on service required
refuse enrolment for this service
refer enrolment request for decision, depending on service required
gateway confirms enrolment for this service
appeal against decision

*Figure 7: Scenario S1: the concept of operations for enrolment*

### 5.2.4 Service use

The detailed online learning service is outside the scope of the security architecture. The following paragraph, however, addresses security and process issues that need to be considered.

A key registration and authentication issue for online learning is whether a real-world identity needs to be established. For example, it could be argued that if no certificate were going to be issued on completion of the course, all that was necessary would be a guarantee that the same individual was using the online learning service each time. This would be used both to present the appropriate element of the learning materials, but also to ensure that the correct assignment and test results were given to the individual.

### 5.2.5 Disenrolment on completion of the need for a specific service

After authentication to the government gateway, the client could request that a specific service is removed from the list of available services. The government gateway would remove the specific service and confirm this to the client using the government gateway secure messaging facility. Subsequently, any information relating only to that service held in the directory entry would be archived and removed.

### 5.2.6 Deregistration initiated by the client on completion of need for UKonline services

After authentication to the government gateway, the client could request that the client identifier and password are no longer required. This would lead to a direct revocation request for the client identifier and password (see section 5.2.1). The government gateway would send a confirmation of the revocation to the client using both the government gateway secure messaging facility and post. Post is suggested in addition to the government gateway secure messaging facility because it provides a measure of protection against a denial of service attack by a hacker. Subsequently, the government gateway would archive the client records and remove the account from the gateway.

As an alternative, the client or a third party acting on his or her behalf, could contact the government gateway help desk by, for example, telephone, say that access to the government gateway was no longer required and request revocation of the client identifier and password.

After verification of the revocation request, the government gateway would revoke the client identifier and password. Verification would be based on shared private information (*eg* NI number, date of birth, mother's maiden name) that had been provided to the gateway as part of the enrolment process.

### 5.2.7 Deregistration initiated by the government gateway

If the client identifier is revoked for any reason, the client will not be successful on a subsequent authentication attempt. The government gateway would send a confirmation of the revocation to the client using the government gateway secure messaging facility. The registration and enrolment policy statement will need to include the appeals process for dealing with deregistration initiated by the government gateway.

The government gateway would retain the client records online for a specified period (120 days, say) to allow for the appeals process and further investigations. If the client identifier were not reinstated within this period, the government gateway would archive the client records and remove the account from the gateway. These could be retrieved at any time if the client identifier were subsequently re-instated.

### 5.2.8 Intermediaries and delegate accounts

*Informal*

It is envisaged that, for example, an individual might informally permit a friend or relative to conduct business on his or her behalf, including enrolment for additional e-Government services, by deliberately revealing the client identifier and password. While this is strongly deprecated and is likely to be a breach of the individual's agreement with the service provider, it must be recognised that this will occur. Provision of a password change facility for authorised clients would allow the actual client subsequently to change the password. Equally, this facility also permits the friend or relative to capture the account.

*Intermediary*

There needs to be a concept of operations for allowing an individual to act on the behalf of a friend or relative under, for example, a power of attorney. It is assumed that a power of attorney exists and may require a signed paper document. An electronic power of attorney will require changes to legislation and is outside the scope of this security architecture.

It is assumed that the attorney has already obtained a client identifier and password for the government gateway, and is enrolled for a number of services. It is envisaged that the attorney would present a duly executed power of attorney to the help desk for the government gateway or to a government department or agency offering a required UKonline service, either by mail or in person. The help desk or government department or agency would check the validity of the power of attorney and then either:

a. enable the attorney's current client identifier and password to permit the attorney to enrol for UKonline services on behalf of the donor of the power of attorney; this might take several days so the attorney would be notified by the government gateway secure messaging service or mail that it had been set up; or

b. generate and issue a separate client identifier and one-time password; this would then be either sent to the attorney's address or issued directly to the attorney.

In either case, sufficient information about the donor of the power of attorney will need to be available to the attorney to permit enrolment at the government gateway. Moreover, the enrolment process will need to take into account any restrictions placed on the attorney (*eg* the attorney might not be permitted to submit a tax return).

The government gateway policy on what approach to adopt and under what circumstances needs to be established and documented in the registration and enrolment policy. For example, it might be more convenient for a client to have only one client identifier and password for access to the government gateway. Alternatively, for an UKonline service essentially requiring positive identification in lieu of a personal signature, the use of separate client identifiers and passwords would be preferable.

*Delegate account*

There needs to be a concept of operations for allowing an organisation (*eg* accountants or law firm) to act on behalf of an individual. It is assumed that the individual has explicitly authorised the organisation to act on his or her behalf. It is envisaged that normally the organisation would already be registered with a number of client identifiers and passwords available.

An individual would need to be identified to at least the standard required for registration and enrolment of the individual for the equivalent personal service. This means that the organisation would need to request appropriate evidence from the individual and check it with information available via the government gateway.

For UKonline services, the organisation will need to manage the access of their staff and record which particular individual carried out a particular transaction for a specific individual. One approach at this level of authentication would be to apply a reference containing a unique identifier for the staff member.

Some UKonline services will require an individual to sign a submission sent on his or her behalf (*eg* as for a personal tax return). At level 1 authentication, this is essentially supported for personal use by having a unique client identifier for the individual. Possible approaches for consideration are:

a. the individual receives an electronic version of the submission, prints out and signs a printed signature page which is then returned to the organisation, for transmission by mail to the relevant government department or agency;

b. the individual receives a paper version of the submission with a signature page; the individual signs the signature page which is then mailed to the organisation, for transmission by mail to the relevant government department or agency;

c. a client identifier and password are issued to the organisation for each individual for which it acts.

## 5.3 Implementation approach

The implementation approach here is to use standard Internet technology and architectures appropriate for each of the access channels. For example, it is envisaged that Secure Socket Layer (SSL) would provide the underlying secure connection for implementing the various security primitives.

# 6. S2: interacting with the Inland Revenue

## 6.1 Introduction

This section sets out the concept of operations and implementation approach for scenario S2: interacting with the Inland Revenue. The security requirements for this scenario are set out at annex E.

The scenario requires that level 2 authentication services be used. The requirement at level 2 is for clients to identify themselves to the system by presentation of a credential (which will preferably be a digital certificate). Clients will demonstrate their right to that credential by, in the case of digital certificates, a private key and using a password or biometric measure.

For the purposes of this scenario, it is assumed that the client will have a digital certificate held within a smartcard. The smartcard has a Personal Identification Number (PIN) known only to the client. Presentation of the PIN demonstrates the client's right to the smartcard. Annex F sets out the assumptions made concerning digital certificates and smartcards.

It is envisaged that the digital certificate / smartcard would be issued by an approved third party RA (*eg* a bank or building society) after an appropriate registration process. Channel providers (for example, iDTV or mobile telephone service providers) may also carry out enrolment at the government gateway if they have approved procedures. The *tScheme* industry self-regulation body is an appropriate UK approver. Production and management of certificates would be the responsibility of a CA. It is assumed that Government and the provider of the digital certificate / smartcard have reached an agreement on transfer of liabilities.

For the purposes of this scenario, it is assumed that registration would normally only involve the production of appropriate documentary, or other, evidence by mail, e-mail or on-line rather than an individual attending at the RA's premises in person. This will allow the RA to establish the validity of the claimed identity, and the client's right to that identity. The evidence required to establish identity at the various levels of trust is set out in the authentication framework, and aligned with the *tScheme* profiles.

Organisations may also operate local registration of delegates by arrangement with the CA.

In the case of businesses, identity issuers need to validate the identity of the organisation, but must also verify the identities of registrants claiming to represent the organisation, and that these registrants have authority to act on behalf of the organisation in a specific role.

The client is authenticated for access to services by using the challenge / response mechanism (see annex F) and by checking the validity of the certificate with the CA.

Digital certificates will expire and can be revoked. The CA maintains a certificate revocation list containing details of revoked certificates.

A client may choose to have a number of different digital certificates / smartcards and use them to enrol for different subsets of available UKonline services. A client may also have different digital certificates / smartcards to undertake separate roles (*eg* for professional and personal use). These separate client identifiers would not be associated with each other unless there was a specific legal need.

For the purposes of this scenario, it is assumed that the identity of the government gateway needs to be formally established.

## 6.2 Concept of operations

### *6.2.1 Registration*

*Figure 8* overleaf provides the concept of operation for registration for scenario S2.

The client selects a third party RA and then provides initial registration information. This would normally include the client's name, date of birth, address, telephone number, e-mail address together with documents providing evidence of the client's identity and address (*eg* a recent utility bill, bank statement *etc*). The RA might also request necessary further information to support the identity of the client.

The RA would carry out appropriate checks on the information provided (*eg* check against the electoral register) or crosscheck the provided information against records held on the government back-office computer. If the checks are positive, the RA will request that the CA generates and issues a smartcard and a one-time PIN and mails them separately to the client at his or her stated home address. The latter provides a measure of protection against spoofing of the identity.

If the checks were negative, the RA would ask the client to confirm information already provided and possibly to provide further information, depending on the detailed registration and enrolment policy. Finally, if the checks were still negative, the RA could refuse registration. The concept of operations allows the client to appeal against this decision. Again, the detailed registration and enrolment policy would need to be established by the RA and agreed with the government.

The client might wish to change his or her PIN, if the original PIN had been forgotten. After appropriate checks on the client's identity, the RA would generate and issue a new one-time PIN and mail it to the client's address.

The concept of operations also provides for revocation of the smartcard / digital certificate. This would be used, for example, if the client decided that access to the government gateway was no longer required, if it subsequently became known that the client's identity was incorrect or if the client informs the RA that the smartcard / digital certificate has been compromised or lost. In the latter cases, after appropriate checks on the client's identity, the RA would generate and issue a new smartcard / digital certificate and one-time PIN and mail them separately to the client's address. Again, the detailed registration and enrolment policy would need to be established by the third-party RA.

In the event of a revocation, the CA would undertake the revocation and would mail a confirmation of the revocation to the client's address and inform the RA. This would help ensure the validity of the revocation request.

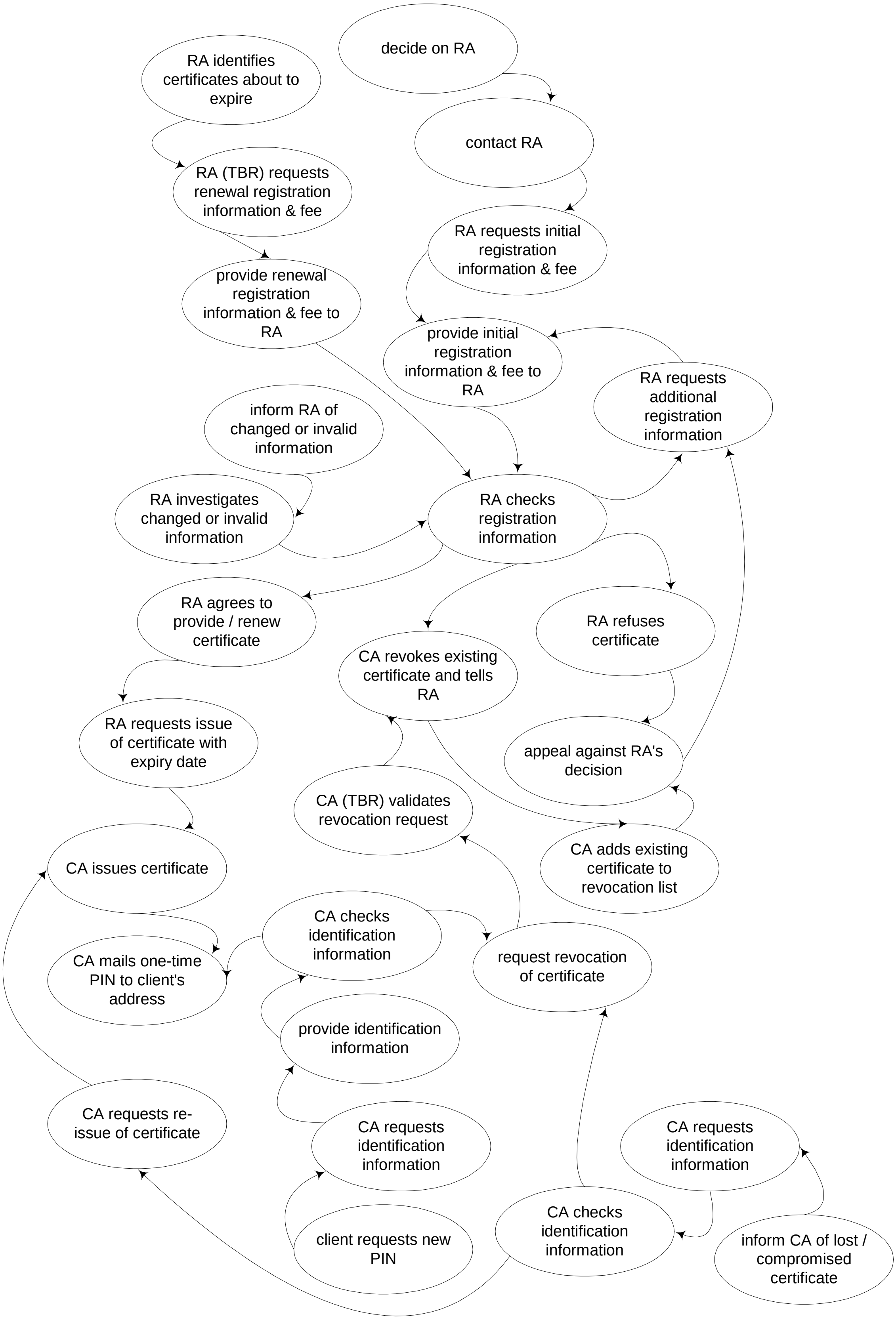

decide on RA
RA identifies certificates about to expire
contact RA
RA (TBR) requests renewal registration information & fee
RA requests initial registration information & fee
provide renewal registration information & fee to RA
provide initial registration information & fee to RA
RA requests additional registration information
inform RA of changed or invalid information
RA investigates changed or invalid information
RA checks registration information
RA agrees to provide / renew certificate
RA refuses certificate
CA revokes existing certificate and tells RA
RA requests issue of certificate with expiry date
appeal against RA's decision
CA (TBR) validates revocation request
CA adds existing certificate to revocation list
CA issues certificate
CA checks identification information
request revocation of certificate
CA mails one-time PIN to client's address
provide identification information
CA requests re-issue of certificate
CA requests identification information
CA requests identification information
client requests new PIN
CA checks identification information
inform CA of lost / compromised certificate

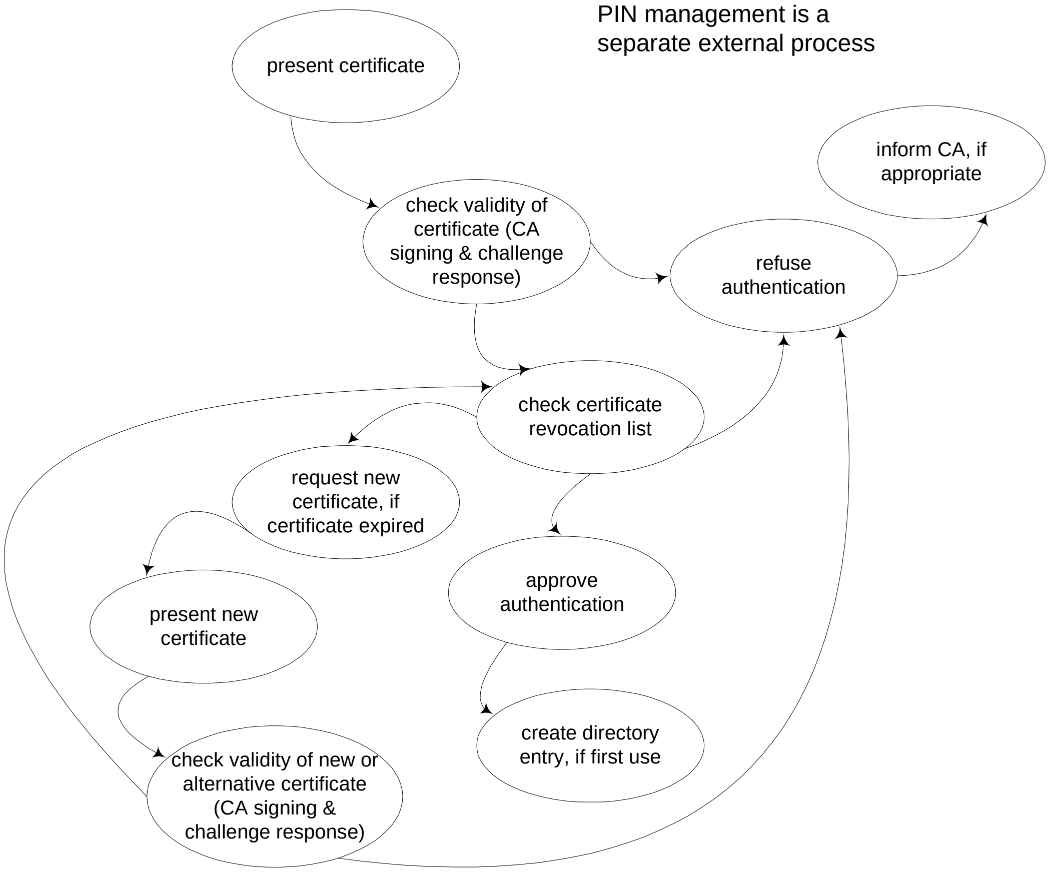
*Figure 8: Scenario S2: the concept of operations for registration*

The overall registration management function is not shown. This would measure and monitor performance information and initiate appropriate management actions to ensure that management objectives and client expectations are managed and met.

It is assessed that the RA would need to establish a help desk to support clients undertaking registration. This could be supported by e-mail and / or telephone.

### 6.2.2 Enrolment at the government gateway

*Figure 9* below provides the concept of operation for enrolment at the government gateway for scenario S2. After validating the smartcard / digital certificate using the PIN, the client presents the smartcard / digital certificate to the government gateway. The gateway checks the validity of the authentication request by using the challenge / response mechanism (annex F) and checking whether the digital certificate is currently valid by accessing the appropriate Certificate Revocation List (CRL), and not been revoked. If the checks are positive, the government gateway authorises the client for access on this occasion.



validation of the certificate
with a PIN is assumed

PIN management is a
separate external process

present certificate
check validity of certificate (CA signing & challenge response)
refuse authentication
inform CA, if appropriate
check certificate revocation list
request new certificate, if certificate expired
present new certificate
approve authentication
create directory entry, if first use
check validity of new or alternative certificate (CA signing & challenge response)

*Figure 9: Scenario S2: the concept of operations for government gateway enrolment*

If the certificate has expired, the government gateway requests presentation of a replacement certificate and rechecks the validity of the authentication request. If the checks are positive, the government gateway updates the list of valid certificates for the client.

It is assumed that the CA is responsible for providing the means to allow the client to validate the smartcard / digital certificate and to set and change the PIN. This process is not shown.

### 6.2.3 Certificate management

Once authenticated the client might wish to use an alternative digital certificate / smartcard, or remove one from use (*eg* the client might change the third party provider for the digital certificate / smartcard). *Figure 10* below provides the concept of operations for this.

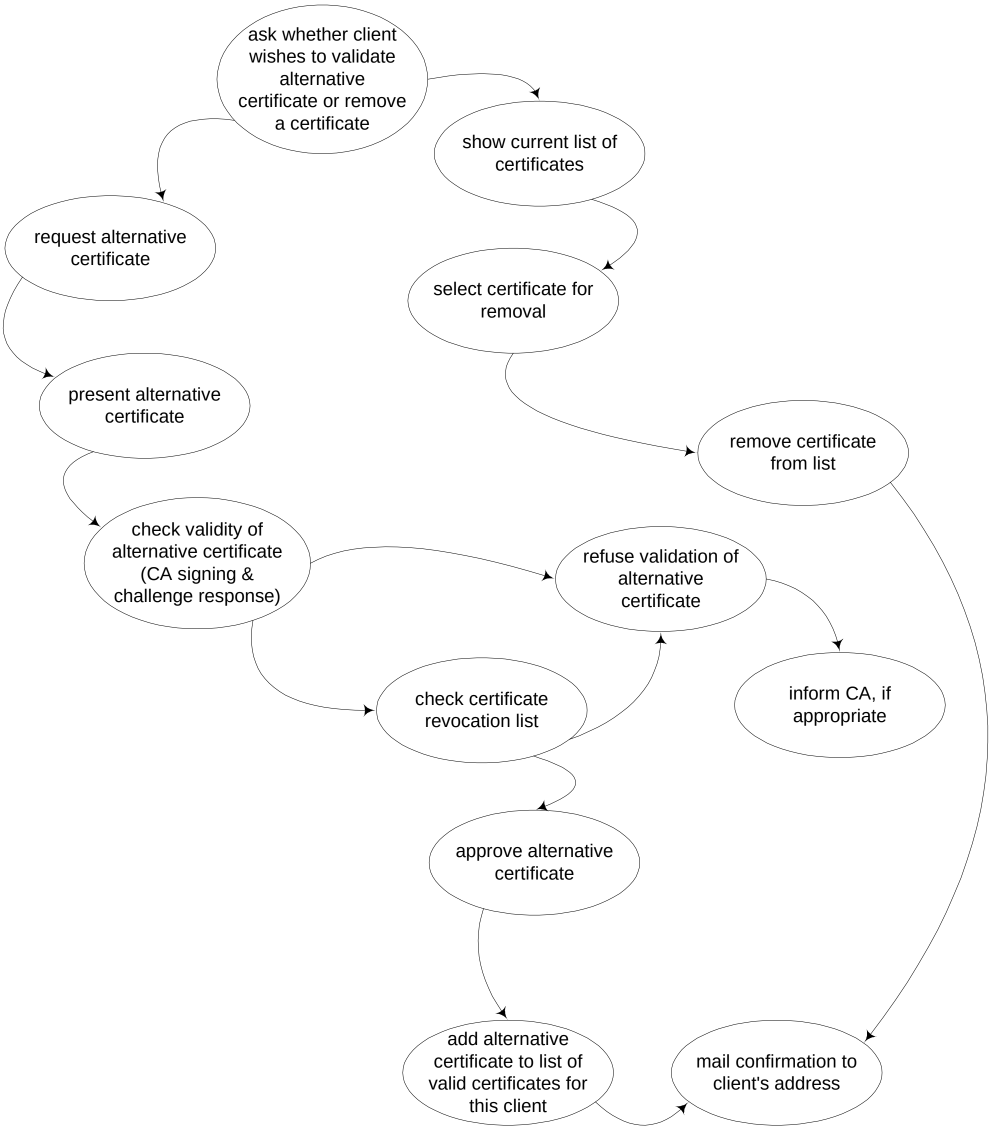

ask whether client wishes to validate alternative certificate or remove a certificate
show current list of certificates
request alternative certificate
select certificate for removal
present alternative certificate
remove certificate from list
check validity of alternative certificate (CA signing & challenge response)
refuse validation of alternative certificate
inform CA, if appropriate
check certificate revocation list
approve alternative certificate
add alternative certificate to list of valid certificates for this client
mail confirmation to client's address

*Figure 10: Scenario S2: the concept of operations for certificate management*

If the certificate management option were selected, the client would be offered the choice of adding an alternative digital certificate / smartcard or removing an existing one.

Adding an alternative digital certificate / smartcard would require the client to validate it with the PIN and then present it to the government gateway. The gateway checks the validity of the digital certificate / smartcard by using the challenge / response mechanism (annex F) and checking whether the digital certificate is currently valid and not been revoked. If the checks are positive, the government gateway associates that the digital certificate / smartcard with the established client. A confirmation of the addition of an alternative digital certificate / smartcard should be sent to the client's registered address.

If the checks fail, the government gateway might, depending on the circumstances, inform the CA. The government gateway registration and enrolment policy needs to address this issue.

Removing a digital certificate / smartcard would require the client to select the appropriate certificate from a list. The government gateway would then remove it. A confirmation of the removal of the digital certificate / smartcard should be sent to the client's registered address.

### 6.2.4 Government gateway authentication

Government gateway authentication is similar to enrolment at the government gateway by a client. The client access channel checks the validity of the government gateway by using the challenge / response mechanism (annex F) and checking whether the government gateway's digital certificate is currently valid and not been revoked. It is envisaged that the client will be able to relate this certificate back to a trusted source. If the checks are positive, the access channel authorises the government gateway on this occasion.

### 6.2.5 Enrolment

*Figure 11* overleaf provides the concept of operations for enrolment for scenario S2. As part of enrolment, the government gateway requests sufficient information from the client to identify uniquely the information corresponding to the client on the relevant government back-office system. The need for this and the acceptable information would be set out in the registration and enrolment policy for the government gateway. As more information provided by the client is verified, the trust in the identity of the client is increased. Enrolment for an UKonline service will require that a one-time password be sent to the client's last registered address. The one-time password would be used only for the first use of the enrolled service.

Initially, the government gateway presents the client with a set of currently enrolled services and services that the client could enrol for at that level of authentication.

If the client selects enrolment in a new service, the government gateway will request any necessary additional information. Once the client has entered this information, the government gateway will search the government back-office records for a match with the provided information, if the check is positive, the government gateway will mail a one-time password to the client's last registered address.

It is envisaged that at the client's request an enrolment could be removed. The government gateway secure messaging facility would be used to send a confirmation.

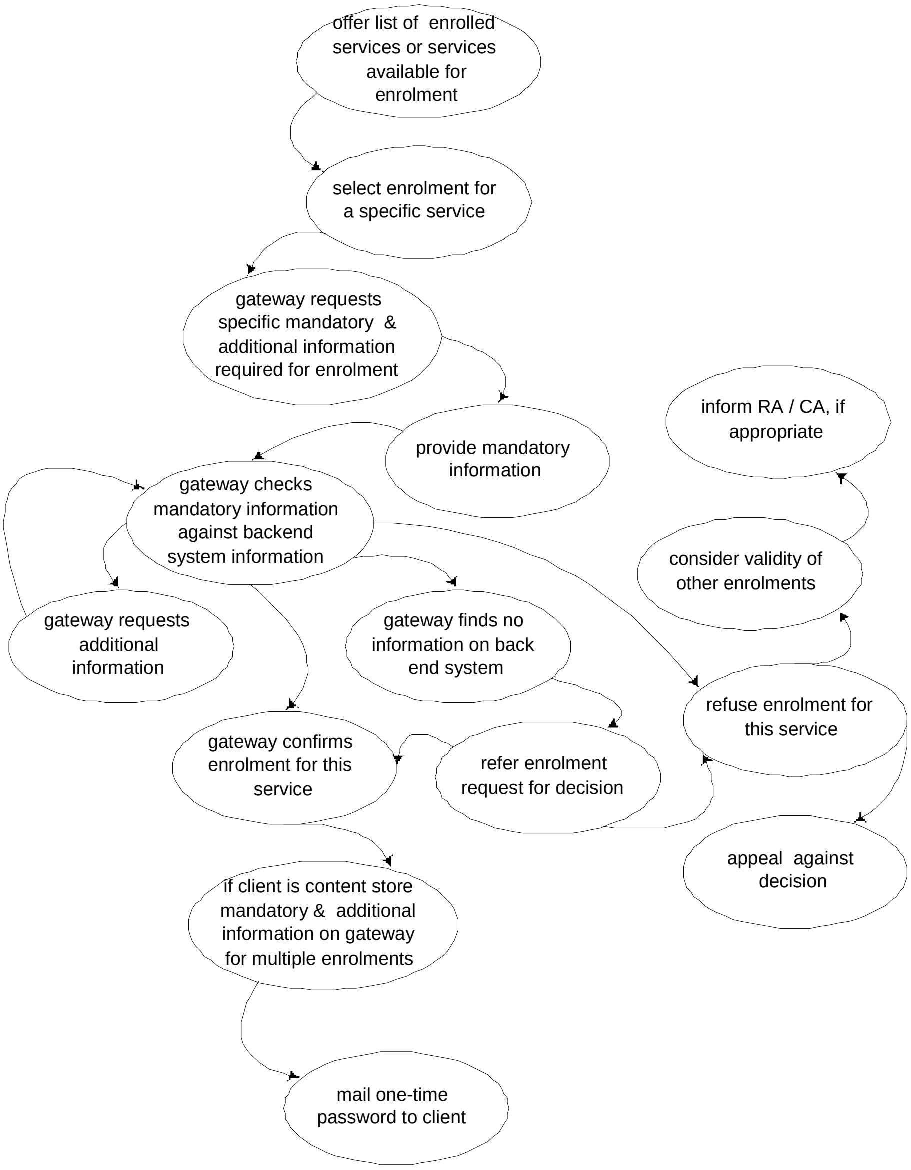
The government gateway would need to establish a helpdesk to resolve enrolment and UKonline service issues. It is envisaged that any registration and authentication issues would be handled by the RA's help desk.

### 6.2.6 Service use

The detailed processes for interaction with the Inland Revenue are outside the scope of the security architecture. The following paragraphs, however, address security and process issues that need to be considered.

It is envisaged that a personal tax return would be signed using the client's private signature key and that responses from the Inland Revenue would be signed using the Inland Revenue's private signature key.

Particular care will be needed to ensure confidentiality of the client's bank or building society information if the client makes a payment electronically. It is envisaged that these would not be stored in the directory.



offer list of enrolled services or services available for enrolment
select enrolment for a specific service
gateway requests specific mandatory & additional information required for enrolment
provide mandatory information
inform RA / CA, if appropriate
gateway checks mandatory information against backend system information
consider validity of other enrolments
gateway requests additional information
gateway finds no information on back end system
refuse enrolment for this service
gateway confirms enrolment for this service
refer enrolment request for decision
appeal against decision
if client is content store mandatory & additional information on gateway for multiple enrolments
mail one-time password to client

*Figure 11: Scenario S2: the concept of operations for enrolment*

### 6.2.7 Disenrolment on completion of the need for a specific service

After authentication to the government gateway, the client could request that a specific service is removed from the list of available services. The government gateway would remove the specific service and confirm this to the client using the government gateway secure messaging facility. Subsequently, any information relating only to that service held in the directory entry would be archived and removed.

### 6.2.8 Deregistration initiated by the client on completion of need for UKonline services

After authentication to the government gateway, the client could request that the UKonline account is no longer required. The government gateway would disable the account by preventing further authentications of the client and would post a confirmation to the client's address. Post is suggested rather than the government gateway secure messaging facility because it provides a measure of protection against a denial of service attack by a hacker. Subsequently, the government gateway would archive the client records and remove the account from the gateway.

As an alternative, the process could be initiated by the client or a third party acting on his or her behalf, could contact the government gateway help desk by, for example, telephone. In this case, the help desk would use manual verification to confirm the validity of the request. This would be based on shared private information (*eg* NI number, date of birth, mother's maiden name) that had been provided to the gateway as part of the enrolment process.

### 6.2.9 Deregistration initiated by the government gateway

If the digital certificate / smartcard is revoked for any reason, the client will not be successful on a subsequent authentication attempt. It is assumed that the CA would send a confirmation of the revocation to the client. The registration and enrolment policy statement will need to include the appeals process for dealing with deregistration initiated by the government gateway.

The government gateway would retain the client records online for a specified period (120 days, say) to allow for the appeals process and potential reinstatement of the digital certificate / smartcard. If the digital certificate / smartcard were not reinstated within this period, the government gateway would archive the client records and remove the account from the gateway. These could be retrieved at any time if the digital certificate / smartcard were subsequently re-instated.

### 6.2.10 Intermediaries and delegate accounts

*Informal*

It is envisaged that, for example, an individual might informally permit a friend or relative to conduct business on his or her behalf, including enrolment for additional e-Government services, by deliberately handing over the digital certificate / smartcard and associated PIN. While this is strongly deprecated and is likely to be a breach of the individual's agreement with the CA, it must be recognised that this will occur. Provision of a PIN change facility by the CA would allow the actual client subsequently to change the password. Equally, this facility also permits the friend or relative to capture the account.

*Intermediaries*

There needs to be a concept of operations for allowing an individual to act on the behalf of a friend or relative under, for example, a power of attorney. It is assumed that a power of attorney exists and may require a signed paper document. An electronic power of attorney will require changes to legislation and is outside the scope of this security architecture.

It is assumed that the attorney has already obtained a digital certificate / smartcard for the government gateway, and is enrolled for a number of services. It is envisaged that the attorney would present a duly executed power of attorney to the help desk for the government gateway or to a government department or agency offering a required UKonline service, either by mail or in person.

The help desk or government department or agency would check the validity of the power of attorney and then enable the attorney's digital certificate / smartcard to permit the attorney to enrol for UKonline services on behalf of the donor of the power of attorney. Initial access would require a one-time password that would be mailed to the attorney's registered address. This might be achieved by presenting the digital certificates / smartcards for both the donor and the attorney. A confirmation would also be mailed to the donor’s registered address. This provides a measure of protection against the theft of a power of attorney.

Sufficient information about the donor of the power of attorney will need to be available to the attorney to permit gateway enrolment and service enrolment for the attorney. Moreover, the enrolment process will need to take into account any restrictions placed on the attorney (*eg* the attorney might not be permitted to submit a tax return).

The government gateway policy on powers of attorney needs to be established in detail (*eg* whether an attorney should have a separate digital certificate / smartcard when acting on behalf of the donor) and documented in the registration and enrolment policy.

*Delegate accounts*
There needs to be a concept of operations for allowing an organisation (*eg* accountants or law firm) to act on behalf of an individual. It is assumed that the individual has explicitly authorised the organisation to act on his or her behalf. It is envisaged that normally the organisation would already be registered with a number of client identifiers and passwords available.

An individual would need to be identified to at least the standard required for registration and enrolment of the individual for the equivalent personal service. This means that the organisation would need to request appropriate evidence from the individual and check it with information available via the government gateway.

For UKonline services, the organisation will need to manage the access of their staff and record which particular individual carried out a particular transaction for a specific individual. One approach at this level of authentication would be to apply a reference containing a unique identifier for the staff member.

Some UKonline services will require an individual to sign a submission sent on his or her behalf (*eg* as for a personal tax return). Possible approaches are:

a. if the individual has a digital certificate / smartcard, the individual would be sent an electronic version of the submission, sign it with his or her private signature key and then return it to the organisation; for transmission by mail to the relevant government department or agency;

b. if the individual does not have a digital certificate / smartcard, the individual would be mailed a copy for signature and return to the organisation for subsequent mailing to the relevant government department or agency.

The government gateway needs to establish the detailed policy for such transactions in conjunction with the relevant government departments and agencies.

## 6.3 Implementation approach

The implementation approach here is to use standard Internet and PKI technology and architectures appropriate for each of the access channels. For example, it is envisaged that Secure Socket Layer (SSL) would provide the underlying secure connection for implementing the various security primitives.

The use of digital certificates and the associated public / private key pairs will allow:

a. digital signing of information submitted by the client or the government gateway to support non-repudiation;

b. encryption of information in transit, over and above SSL;

c. strong authentication to enable access to modify directory information.

# 7. S3: informing a client of the results of medical screening

## 7.1 Introduction

This section sets out concept of operations and implementation approach for scenario S3: informing a client of the results of medical screening. The security requirements for this scenario are set out at annex G.

The scenario requires level 3 authentication services. The requirement at level 3 authentication is for clients to identify themselves to the system by presentation of a digital certificate. This will preferably be held in a secure token, such as a smartcard. Clients will demonstrate their rights to that credential by a private key, and a password or biometric. The system will authenticate clients based on the validity of the public key / private key pairs, and on the validity of the credential.

This corresponds to the assumptions made for scenario S2 (see section 6.1) with the exception that registration, if required, would probably be carried out face-to-face. It is assessed that the concept of operations set out above for scenario S2 applies and so it is not repeated. There are, however, issues arising from the different service use and these are described below.

## 7.2 Concept of operations

### *7.2.1 Service use*

The detailed processes for informing a client of the results of medical screening are outside the scope of the security architecture. The following paragraphs, however, address security and process issues that need to be considered.

There needs to be a concept of ‘guaranteed delivery’ for sending the results of a medical screening to a client, particularly where the client might need urgent medical attention. Use of normal e-mail would not be satisfactory, as it does not guarantee delivery. This might be because of failure of the e-mail system to deliver the message, failure of the client to examine his or her e-mail inbox and failure of the client to take appropriate action. One possible approach is to:

a. send a message to the client using the government gateway secure messaging facility saying that a follow-up appointment is necessary with a selection of times;

b. note that the message has been sent and that the delivery needs to be reviewed at a specified time, depending on the urgency of the follow-up;

c. at the specified review time, resend the mail message and also use post and telephone to try and contact the individual and consider asking the police or social services to follow up, if necessary and appropriate.

Careful consideration will need to be paid to confidentiality and privacy. A particular issue is the policy for allowing an intermediary acting on the client's behalf to receive, or respond to, a secure message.

## 7.3 Implementation approach

The implementation approach here is to use standard Internet and PKI technology and architectures appropriate for each of the access channels. For example, it is envisaged that Secure Socket Layer (SSL) would provide the underlying secure connection for implementing the various security primitives.

The use of digital certificates and the associated public / private key pairs will allow:

a. digital signing of information submitted by the client or the government gateway to support non-repudiation;

b. encryption of information in transit, over and above SSL;

c. encryption of directory information; there are issues here as to whether this should be a government gateway private key or the client's private key.

# A Abbreviations

| | |
|---|---|
| CA | Certification Authority |
| CRL | Certificate Revocation List |
| DPA | Data Protection Act |
| iDTV | interactive Digital Television |
| ISP | Internet Service Provider |
| NI | National Insurance |
| PAYE | Pay as You Earn |
| PC | Personal Computer |
| PIN | Personal Identification Numbers |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| RP | Relying Party |
| SSL | Secure Socket Layer |
| WAP | Wireless Access Protocol |

# B Glossary

The glossary covers the security architecture and is the same as the one in the security framework.

### *B.1.1 Access system*

An access system is an IT system that in conjunction with one or more back-office systems hosts e-Government services. Clients gain access to e-Government services via an access system element. Examples of access systems are the Government Secure Internet (GSI) and the government gateway.

### *B.1.2 Access system registration*

Access system registration is the process in which an access system can establish a credential and present this to the client for authentication of the access system to the client.

### *B.1.3 Access token*

An access token is a (physical) medium that contains a credential, for example a smartcard that contains a digital certificate.

### *B.1.4 Accreditor*

The person responsible for the accreditation of a system or service.

### *B.1.5 Anonymous client*

An anonymous client is one who chooses to reveal no real-world identity during the registration process prior to authentication for a specific transaction. The client may or may not possess a credential. A client possessing a credential, with an associated electronic identity, can be recognised for repeat transactions using that credential. If the client does not need to possess a credential, any resulting transactions could be truly anonymous and untraceable.

### *B.1.6 Assurance*

Assurance is the set of processes and practices to help ensure that e-government services are designed, implemented, configured, maintained and operated in accordance with the security framework.

### *B.1.7 Assurance level*

The assurance level is a measure of assurance matched to security profile defined by the Common Criteria for IT Security Evaluation. This should comply with ITSEC or *tScheme* approval.

### *B.1.8 Authentication*

Authentication is the process by which the electronic identity of a user is asserted to, and validated by, an information system for a specific occasion using a credential issued following a registration process. It may also involve establishing that the user is the true holder of that credential, by means of a password or biometric. A client is required to authenticate their electronic identity every time they wish to engage in an UKonline session.

### *B.1.9 Authorisation*

Authorisation is the granting of rights to access services, information and resources.

### *B.1.10 Back-office system*

A back-office system is the computer system within a government department, agency, local or regional authority or other e-government service provider, which completes a requested service based on data passed from an access system.

### *B.1.11 Business sponsor*

The individual within the government organisation that holds overall responsibility for the service provision and security of an e-government service. The business sponsor works in conjunction with the service provider (who may or may not belong to the same organisation) and accreditor to select, implement and assure appropriate security measures for the service.

### *B.1.12 Certificate Revocation List (CRL)*

A certificate revocation list is a list of certificates that have been withdrawn prior to their normal expiry date.

### *B.1.13 Certification Authority (CA)*

A certification authority issues, manages and revokes digital certificates at the request of Registration Authorities.

### *B.1.14 Challenge response*

Challenge response is a mechanism that is typically used to test whether the recipient of the challenge can be authenticated for a particular service. It can be implemented using PKI techniques.

### *B.1.15 Client*

A client is a person, an organisation, a duly authorised representative of the person or organisation or a process seeking to carry out a transaction with government.

### *B.1.16 Credential*

A credential is a set of information, which is used by a user to establish an electronic identity to a computer system as part of the authentication process. A credential may be associated with ancillary information supporting a client's right to possess that credential (such as a PIN or private signing key). Examples of credentials are client identifiers or a digital certificate held within a smartcard.

### *B.1.17 Credential issuer*

A credential issuer issues, manages and revokes credentials. A Certification Authority is one example of a credential issuer.

### *B.1.18 Credential revocation list*

A credential revocation list is a list of credentials that have been withdrawn prior to their normal expiry date.

### *B.1.19 Directory*

A directory is the set of information that allows an access system to map uniquely between the client's credential and the information (in database terms, the 'primary key') needed to identify the client to the service the client is requesting.

### *B.1.20 Disenrolment*

The process by which a client's right to a particular service is removed.

### *B.1.21 Electronic identity*

An electronic identity is a set of information that uniquely identifies a user to a computer system. Examples of an electronic identity are a username or digital certificate identifier.

### *B.1.22 Enrolment*

Enrolment is the process by which a client obtains authorisation for a specific online service.

### *B.1.23 Government gateway*

The government gateway is a specific example of an access system. It is a hub linking portals and external back-office systems to government back-office systems. Amongst other things, the gateway provides common security services, including client authentication, confidentiality and privacy. Once a client has been authenticated, the government gateway forwards information between the client and appropriate government back-office systems. It co-ordinates transactions on government back-office systems on behalf of the client to support ‘joined-up’ government services. The government gateway also provides a secure messaging facility to allow government departments to communicate with the client. The linkage between a portal and government back-office systems may be asynchronous, or synchronous.

### *B.1.24 Government gateway enrolment*

Enrolment at the government gateway is the process by which a client first registers with a relevant access system by presenting an acceptable credential. The access system will check the validity of the credential and set up a directory entry corresponding to the credential and containing information specific to the client.

### *B.1.25 Government user*

A person or process that interacts with an e-government service from a back-office system or access system (in any capacity). This includes third parties involved in the provision of e-government services.

### *B.1.26 Practice statement*

A practice statement is a statement, published by a registration service provider or a credential issuer, setting out its practices in registering clients and issuing and managing credentials.

### *B.1.27 Pseudonymous client*

A pseudonymous client is one who chooses only to reveal a pseudonym as part of the registration process prior to authentication for a specific service. The client may or may not possess a credential. A client possessing a credential, with an associated electronic identity can be recognised for repeat transactions using that credential. If the client does not need to possess a credential, any resulting transactions could be truly pseudonymous and untraceable.

### *B.1.28 Real-world identity*

A real-world identity is a set of attributes (*eg* name, date of birth, national insurance number), which uniquely discriminates between users. An entity can possess only one real-world identity (*eg* a person or an organisation). However, a single real-world identity may be used in conjunction with different roles. Depending on the transaction, a user may be required to reveal their real-world identity or may be permitted to use a pseudonym or remain anonymous.

### *B.1.29 Receipt*

A receipt provides evidence for a party in a transaction that can be used at a later date to confirm that a specific element of the transaction has been completed.

### *B.1.30 Registration*

Registration is the process by which a user gains a credential such as a username or digital certificate for subsequent authentication. This may require the client to present proof of real-world identity (such as birth certificate, passport) and/or proof of other attributes depending on the intended use of the credential (*eg* proof that an individual works for a particular organisation). Registration can be associated with a real-world identity or can be anonymous or pseudonymous.

### *B.1.31 Registration Authority*

A registration authority (RA) is the organisation that validates evidence both of a user's real-world identity and of the client's right to that real-world identity. If the identification is successful, the client will usually be supplied with a credential for subsequent authentication (either directly, if the RA is also a credential issuer, or by another body such as a Certification Authority).

### *B.1.32 Registrant*

A registrant is a person, an organisation or representative of a person or an organisation seeking to establish their identity and obtain a credential from an issuer.

### *B.1.33 Registration and enrolment policy*

It is envisaged that there would be a detailed registration and enrolment policy statement for access systems that provide client access. This would include, for example, the clients entitled to register, the appropriate type of registration for each UKonline service, information that needs to be collected from a client during registration and enrolment, the appeals process, acceptable credentials and the relationship between a credential provider and the government.

### *B.1.34 Relying Party*

The relying party trusts a credential to associate an electronic identity with a client. The relying party is often the organisation that is responsible for carrying out the government service, and hence relies upon a credential as part of authorising a client. For example, the Inland Revenue is the relying party for a client's Income Tax Self-Assessment. However, clients may also be relying parties if they rely on a government credential to assure themselves that they are really dealing with government.

### *B.1.35 Risk*

Risk is a function of asset value and the impact and likelihood of threat and vulnerabilities.

### *B.1.36 Risk assessment*

A risk assessment is an assessment of threats to, impact on and vulnerabilities of information and information processes and the likelihood of their occurrence.

### *B.1.37 Roles*

A client may assume one or more roles in the client's interaction with government. For example, a person may simultaneously be both an employee and an employer. Similarly, government users may assume a number of roles in their interaction with e-government services.

### *B.1.38 Security domain*

A security domain is a set of equipments or security processes within a specific management regime.

### *B.1.39 Service provider*

The service provider is an organisation responsible for the provision of a specific e-government service. The service provider might merely operate the service using its own or government-owned equipment, or it might also design and develop the service.

The service provider must ensure that the service and relevant systems are compliant with the e-government security framework, in conjunction with the accreditor and the business sponsor.

### *B.1.40 Threat*

A threat is the likelihood that an attacker will attempt and has the capability to exploit a vulnerability to breach security.

### *B.1.41 Trust service provider*

A trust service provider is an organisation that provides trust services. Trust service providers include registration authorities, since they provide a measure of trust in the asserted real-world identity of a client.

### *B.1.42 UKonline*

As a brand, UKonline refers to the provision of government services by electronic means. The service provider could be, for example, one or more of a central government department, a government agency, a local authority or a private sector organisation acting on behalf of local or central government.

### *B.1.43 UKonline citizen portal*

The UKonline citizen portal is the current electronic interface between clients and the government. It is accessed through Internet-based technologies, uses websites to bring information together and a gateway to provide a common interface to the government back-office systems operated by government departments and agencies. The UKonline citizen portal also presents publicly available information. The UKonline citizen portal is one of a number of portals that provide access to UKonline services.

### *B.1.44 UKonline service*

A UKonline service is any service that a client can access electronically within the UKonline brand.

### *B.1.45 Unpublished data*

Unpublished data is information that is likely to be known only to the credential holder and the service provider: for example, information about a previous transaction.

### *B.1.46 User*

A user is a person or process that interacts with an e-government system (in any capacity).

### *B.1.47 Vulnerability*

A vulnerability is a feature of a system which, if exploited by an attacker, would enable the attacker to breach security.

# C S0: accessing publicly available information

## C.1 Assessment of security requirements

### *C.1.1 Registration and authentication services*

For access to publicly available information, there is no need to identify the client reliably. The client would require a valid e-mail address for any information returned by e-mail, but this could be, for example, an anonymous or pseudonymous (*eg* a ‘hotmail’ address). Accordingly, this is assessed as requiring level 0 registration and level 0 authentication services.

### *C.1.2 Trust services*

There would be no lasting consequential loss or financial impact arising from failure to complete the access to the publicly available information. The client would repeat the information request or abandon the attempt. It is anticipated that any claim for damages arising from a failure to gain the required information would not succeed. Accordingly, this is assessed as requiring level 0 trust services.

### *C.1.3 Confidentiality services*

There is no private information content and it is assessed as requiring level 0 confidentiality services.

### *C.1.4 Network defence services*

An electronic attack on the service possibly leading to the delivery of defaced information could have a minor inconvenience impact on the client. Moreover, there might be minor embarrassment caused to the government’s reputation regarding the provision of e-Government services. Accordingly, the scenario is assessed as requiring level 1 network defence services.

### *C.1.5 Business services*

Failure of the service is unlikely to lead to the release of personal, financial or commercially sensitive information to third parties or assist in the commission of, or hinder the detection of, serious crime. However, failure or unavailability of the service could result in minor inconvenience to the client or minor embarrassment to the government’s reputation regarding the provision of e-Government services. Accordingly, it is assessed as requiring level 1 business services.

# D S1: a client interacting with an online learning system

## D.1 Assessment of security requirements

### *D.1.1 Registration and authentication services*

If successful completion of the online learning activity results in the issue of a recognised certificate, there would need to be positive identification of the student's real-world identity. The client would require a valid e-mail address for any information returned by e-mail, but this could be, for example, an anonymous or pseudonymous (*eg* a 'hotmail' address).

Based on the assumption that fraudulently obtaining the recognised certificate would only lead to minor financial loss by a third party (*eg* an employer), this scenario is assessed as requiring level 1 registration and level 1 authentication services.

In any practical application, an organisation offering online learning services would need to consider whether any certificate obtained was significant enough to justify higher levels of registration and authentication. For example, it might be inappropriate to offer social service qualifications completely online. Moreover, consideration would also need to be given to whether the client once registered would use a substitute to complete assignments *etc*.

If no recognised certificate is issued, the client could choose to be anonymous or to use a pseudonymous identity. Accordingly, for this case, the scenario requires level 1 authentication and level 0 registration services.

### *D.1.2 Trust services*

The relationship between the parties is essentially of a personal nature and failure to complete a transaction (*eg* returning an assignment on time) or confusion over the content would have a minor nuisance impact on one or more of the involved parties. Accordingly, this is assessed as requiring level 1 trust services.

### *D.1.3 Confidentiality services*

The information content is client specific but has minimal sensitive content. The impact of public disclosure would at worst be minor inconvenience or embarrassment, or might lead to a poor perception of system security for e-Government. Accordingly, it is assessed as requiring level 1 confidentiality services.

### *D.1.4 Network defence services*

An electronic attack on the service possibly leading to the delivery of defaced information could have a minor inconvenience impact on the client. Moreover, there might be minor embarrassment caused to the government's reputation regarding the provision of e-Government services. Accordingly, the scenario is assessed as requiring level 1 network defence services.

### *D.1.5 Business services*

The failure of the service is unlikely to lead to the release of personal, financial or commercially sensitive information to third parties or assist in the commission of, or hinder the detection of, serious crime. However, failure or unavailability of the service could result in minor inconvenience to the client or minor embarrassment to the government's reputation regarding the provision of e-Government services. Accordingly, it is assessed as requiring level 1 business services.

# E S2: interacting with the Inland Revenue

## E.1 Assessment of security requirements

### *E.1.1 Registration and authentication services*

Interacting with the Inland Revenue is of an official nature. Failure to undertake the transaction might be interpreted as a statutory infringement that might incur a significant penalty or significant loss of tax revenues. Moreover, the information is of a personally sensitive nature and misappropriation of a credential might result in the release of personally sensitive information, or might lead to significant damage to the client's reputation. Accordingly, for this scenario, level 2 registration and level 2 authentication services are required.

### *E.1.2 Trust services*

Interacting with the Inland Revenue is of an official nature. A perceived failure to undertake the transaction might be interpreted as a statutory infringement that might incur a significant penalty. Accordingly, this is assessed as requiring level 2 trust services.

### *E.1.3 Confidentiality services*

The information content involves private information that could be regarded as sensitive, and where the impact of disclosure might result in significant financial loss or damage to the reputation or standing of the client. Accordingly, it is assessed as requiring level 2 confidentiality services.

### *E.1.4 Network defence services*

The service is of an official nature, compromise of which by electronic means (*eg* by hacking leading to changing of client-entered information) may be interpreted as a statutory infringement that may incur a penalty or cause significant loss of tax revenues. Accordingly, the scenario is assessed as requiring level 2 network defence services.

### *E.1.5 Business services*

Failure to make the service available might be interpreted as a statutory infringement that might incur a penalty or significant loss of tax revenues. Failure of services might result in the release of personally confidential information or material damage to the client's reputation or standing. Accordingly, it is assessed as requiring level 2 business services.

# F Assumptions for digital certificates and smartcards

The following paragraphs set out the assumptions made for digital certificates and smartcards and outlines the challenge /response mechanism.

### *F.1.1 Availability of digital certificates*

Digital certificates, contained in a smartcard, will be widely available to both businesses and the public. It is envisaged that particular organisations (*eg* banks, building societies, the Post Office *etc*) would act as RAs for certificates for use in its e-Business processes. As a benefit to the customer, these smartcards could also be used elsewhere, including UKonline, subject to agreement between the parties on transfer of liabilities.

A smartcard has an associated PIN, which is used to ensure that the client is the legitimate owner of the smartcard.

An individual or a business might have several digital certificates.

### *F.1.2 Contents of a digital certificate*

The digital certificate is assumed to follow X.509. Table F-1 categorises classes of certificate by name attributes and lists their applicability.

| Class | Name | Used for authentication level | Checking | Applicable scenario |
|---|---|---|---|---|
| 1 | Anonymous, pseudonym, actual name or business name | 0 | None | S1 |
| 2 | Actual name and / or organisation name | 1 | Remote checking of evidence | S2 |
| 3 | Actual name and / or organisation name | 2 | Face-to-face checking of evidence | S3 |

Table F-1: Summary of name attributes for certificate classes

### *F.1.3 UKonline policy on use of digital certificates*

UKonline will accept an appropriate digital certificate, providing it contains an X.509 certificate issued by an authorised CA with whom UKonline has an agreement to allow UKonline access to relevant CA information bases (*eg* the certificate revocation list).

UKonline will not accept any digital certificate as guaranteed evidence of identity because:

names are not by themselves a guarantee of a unique individual;

the digital certificate and / or the RA may not have needed to collect appropriate personal information for enrolment on a particular service and / or may not be permitted to release the information;

a digital certificate may not necessarily contain the client’s name;

privacy issues in the UK preclude the introduction of unique identifiers for individuals or the use in a single certificate of a combination of existing information sufficient to provide a unique identity (*eg* name, date of birth, NI number, address).

In addition, RAs and CAs wish to limit their liabilities. Accordingly, an RA might be unwilling to accept any liability for use of its digital certificate as a means of identification for access to, say, UKonline services involving, for example, significant financial transactions.

UKonline policy for UKonline services that require a name for enrolment is thus to:

check the certificate validity and request further information to check against available information on the appropriate UKonline government back-office system (*eg* asking for a name (if there is no name in the certificate) NI number and address and checking this against the individual’s PAYE records) at first presentation of a digital certificate to UKonline for enrolment;

not allow immediate access to a requested service on enrolment; the approach is to send a one-time password to the individual or organisation at the last known address recorded in the government back-office system;

check the certificate validity and then request and check the one-time password at the next presentation of the digital certificate for the particular enrolled service; this approach helps to establish trust in the binding between the digital certificate and the individual / organisation;

allow access to the enrolled UKonline service on subsequent presentation of the digital certificate, provided it is still valid.

UKonline policy for UKonline services that do not require a name for enrolment is to allow access to the service if the digital certificate is valid.

### *F.1.4 UKonline assumptions on smartcards*

A smartcard is assumed to provide a client with the following:

an X.509 digital certificate;

a public / private key pair for encryption of information sent to the client;

a public / private key pair for digital signing of information created by the client;

identifiers for the relevant encryption and / or signing methods used.

Good practice[25] suggests the key pairs used for signing and encrypting should be distinct. This is true even when the algorithm used, i.e. RSA, supports both encryption and signing with a single key pair.

### *F.1.5 Challenge / response mechanism*

This mechanism is typically used to test whether the owner of a digital certificate / smartcard can be authorised for a particular service.

The UKonline service provider issues a challenge as to the client's identity. The challenge comprises a number selected at random. This number is signed with the client's private signature key and returned. The UKonline service provider then uses the known public signature key to decrypt the number. If the original number is unchanged, the client has the appropriate private / public key pair and can then be duly authorised.

### *F.1.6 Certificate revocation*

CAs maintain an accessible Certificate Revocation List (CRL) that contains details of certificates that have been revoked. As part of authentication, the certificate revocation list should be checked to ensure that the certificate is still valid.

[25] This is because a mechanism for backup and recovery of the private key is appropriate for an encryption key, but not for a signing key.

# G S3: informing a client of the results of medical screening

## G.1 Assessment of security requirements

### *G.1.1 Registration and authentication services*

Informing a client of the results of a medical screening is of an official nature. Moreover, mistaken identity may have significant impact on the health or safety of the client and possibly others. Accordingly, for this scenario, level 3 registration services and level 3 authentication services are required.

If the client can choose to remain anonymous or use a pseudonym, level 0 registration services would be required. However, the need to ensure that the same individual who underwent the screening would also receive the results means that level 3 authentication services would be required.

### *G.1.2 Trust services*

Informing a client of the results of a medical screening is of an official nature. Loss of integrity for the transaction might affect the health or safety of the client and possibly others. Accordingly, this is assessed as requiring level 3 trust services.

### *G.1.3 Confidentiality services*

The information content involves private information that could be regarded as sensitive, and where the impact of disclosure might result in substantial personal distress. Accordingly, it is assessed as requiring level 3 confidentiality services.

### *G.1.4 Network defence services*

The service is of an official nature, compromise of which by electronic means (*eg* by hacking leading to changing the screening result) may have a substantial impact on the safety or health of the client. Accordingly, the scenario is assessed as requiring level 3 network defence services.

### *G.1.5 Business services*

Failure to make the service or screening results available might affect the health or safety of individuals. Accordingly, it is assessed as requiring level 3 business services.

Online copies of this document will be made available at: www.govtalk.gov.uk

Office of the e-Envoy, Stockley House, 130 Wilton Road, London, SW1V 1LQ