CABINET OFFICE

Office of the *e-Envoy*

Leading the drive to get the UK online

*delivering* UK online

# Registration and Authentication

## e-Government Strategy Framework Policy and Guidelines

Version 3.0
September 2002

# Contents

# 1. Introduction

## 1.1 Ownership and maintenance

The e-Government registration and authentication framework policy and guidelines document is one of a series 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.

This document builds on the e-Government security policy[2] that sets out the e-Government security requirements. It specifically addresses those security requirements related to the provision of registration and authentication services to support access to e-Government services.

This version of the document incorporates comments received after a public consultation exercise.

## 1.2 Terminology

The following definitions are used in connection with the provision of e-Government services:

a) **Registration**: This is the process by which a user[3] gains a credential such as a username or digital certificate for subsequent authentication. This may require the user 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) **Authentication**: The process by which the electronic identity[4] 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 in order to use some of the services available through UKonline.

The meaning ascribed to these and other specific terms in the document is provided in the glossary in the overarching security framework.

---

1 *Modernising Government white paper*.

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

3 Throughout this document set, user is defined as a person or process that interacts with an e-Government system. This is a generic term that encompasses clients, and government users in any capacity.

4 Throughout this document, a distinction will be made between an *electronic identity*, which is used to denote a set of information that uniquely identifies a user to a computer system (such as username or digital certificate) and a *real-world identity*. The electronic identity will necessarily belong to a real-world identity (a person, an organisation, a representative of the person or organisation or a process), but this real-world identity need only be revealed if it is necessary for the transaction. The categories of real-world identification are discussed in section 2.5.

A list of abbreviations is also provided at annex A.

## 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.

It is also relevant to security authorities that may use this document to assess the suitability of offered solutions and accredit them for operational use.

## 1.4 Background

Government and those it deals with have mutual obligations relating to the use of e-Government services. In particular:

a) government must:

   i. release personal or commercially sensitive information only against reliably verified authority;

   ii. provide services and benefits only to those entitled to receive them;

   iii. communicate clearly to clients the criteria for access to particular services; and

   iv. when it is under the government's control, protect clients against misuse of their authority.

b) government and those it deals with must be bound by declarations they have made and instructions they have given.

Clients must also be able to identify the government systems and personnel with which they deal. Business sponsors must recognise and provide for this need, at a level appropriate to the transaction. Use of PKI techniques can provide this functionality in the longer term.

Gaining and maintaining the confidence and trust of individuals, businesses and other organisations will be one of the key success factors for the provision of e-Government services. Clients[5] will need to be confident that a service is secure and that their privacy is being maintained.

Registration and authentication are two necessary activities for gaining and maintaining trust and are the subject of this document.

[5] 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.

## 1.5 Objective

This document is intended to set out a number of trust levels for registration and authentication in e-Government transactions.

Current guidance on the use of registration and authentication services in the context of e-Government services is set out in the companion security architecture document[6].

## 1.6 Scope

This document is concerned with the registration and authentication of citizens and organisations seeking to access government services electronically. It applies in circumstances where government needs to have trust in the identity (real-world or otherwise) and authority of those it is dealing with to ensure that there is no breach of privacy or confidentiality, theft/misuse of data, or other harm. The framework includes those cases where anonymous or pseudonymous access is acceptable.

Business sponsors must also consider the role of registration, authentication, access control and user access management in the context of government users. The exact requirements may differ from those that relate to clients, since other aspects of security (*eg* physical and procedural) may be applicable.

The applicability of the framework to transactions where government is simply receiving payments *via* electronic media in exchange for the provision of goods, services or information to consumers, for example where a government department wishes to sell goods over the Internet and sets up a web site accepting credit card payments, needs to be examined on a case by case basis. It is likely that in these circumstances, good commercial practice should be appropriate.

## 1.7 Organisations affected by this document

This framework applies to all electronic transactions carried out by or on behalf of government where there is a need for registration and/or authentication. It is intended to ensure that all government bodies, and organisations providing services on their behalf, carry out registration and authentication in a consistent manner when providing services electronically.

For most electronic transactions, government will accept credentials provided, or partially provided, by accredited third parties, which will register clients and issue them with credentials enabling them to authenticate themselves in subsequent transactions.

Central government departments and agencies **must comply** with this framework in respect of electronic transactions. They shall, when introducing an electronic transaction:

a) follow the guidance in this framework in order to allocate the transaction to both a registration level and an authentication level;

b) follow the guidance in this framework to deliver appropriate registration and authentication processes and functionality for the assigned levels;

---

[6] The latest version of *e-Government strategy: security architecture.* Available at http://www.e-envoy.gov.uk

c) note the advice on data protection contained in this framework, the more general work on this subject which forms part of the e-Government strategy, and their obligations under data protection legislation; and

d) ensure that they have considered all the risks set out in section 5 of this paper, and instituted adequate countermeasures. Some of these risks may not be directly related to service providers but rather to trust service providers; in which case the consideration and institution is satisfied in an appropriate choice of trust service provider.

It is strongly recommended that other public sector bodies adopt the recommendations of this framework in respect of transactions that they conduct with businesses and the public or which are conducted on their behalf.

## 1.8 Relationship to other framework documents

The over-arching e-Government security policy framework document defines the following service control objectives. The means of achieving these objectives are considered in detail in this and other framework documents.

The documents form a complete set and it is strongly suggested that they should be read together. The overarching security policy framework document also provides guidance on how the documents should be used for the process of service security requirements specification and accreditation.

The e-Government registration and authentication framework document (this document) addresses the following objectives:

a) OS1 – Effective user identification and authentication;

b) OS2 – Effective user registration;

c) OS3 – Effective access control;

d) OS4 – Effective user access management.

The trust services framework document[7] addresses the following objectives:

a) OS5 – Non repudiation;

b) OS6 – Evidence of receipt;

c) OS7 – Trusted commitment service;

d) OS9 – Integrity.

The confidentiality framework document[8] addresses the following objective:

a) OS8 – Privacy and confidentiality.

---

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

The business services framework document[9] addresses the following objectives:

a) OS10 – Service availability;

b) OS11 – Information availability;

c) OS13 – Effective audit and accounting.

The network defence framework document[10] addresses the following objective:

a) OS12 – Service protection.

The assurance framework[11] document addresses the means by which trust in the implementation of security elements can be assured.

## 1.9 Availability of advice

In the first instance, advice on the application of the registration and authentication framework may be obtained from the Office of the e-Envoy[12].

CESG[13] is the national technical authority on information security and may be consulted for further advice and assistance on technologies, measures and products to meet these requirements.

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

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

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

12 http://www.e-envoy.gov.uk.

13 Telephone 01242 237323 or *via* http://www.cesg.gov.uk.

# 2. Summary of government's approach to registration and authentication

## 2.1 Introduction

This section sets out the approach to the provision of all or part of e-Government services by third parties, including obligations on third parties for registration and authentication. It also sets out possible trust models for registration and authentication.

An overarching operations concept for a client engaging in e-Government transactions in the context of the current Government Gateway, and with the current limitations on the use of PKI, is given in the Security Architecture.

## 2.2 Third party participation in provision of e-Government services

### *2.2.1 Provision of registration services by third parties*

Government will encourage the provision of registration services by a variety of bodies, including local authorities and the private sector, and will seek to make use of these services wherever possible. Government welcomes the *tScheme* for accreditation of trust service providers, which has been set up by the Alliance for Electronic Business (AEB), and will seek to work closely with the AEB and other relevant bodies to agree detailed standards for registration and authentication services for government transactions.

Any third party providing registration services to support e-Government transactions must be approved under a scheme recognised by the UK government such as *tScheme*.

### *2.2.2 Third party service delivery*

The Modernising Government white paper makes clear the government's intention to work in partnership with Local Authorities, the voluntary sector, and with third-party delivery channels such as the Post Office and private sector companies. Where third-party service providers are conducting transactions on the government's behalf, they will be required to perform registration, authentication and enrolment[14] of the clients they deal with, and, where appropriate, of government users, to the same standards as government itself would. Government will in turn accept transaction data from those delivery channels, who will certify that they have carried out the transaction to the agreed standard. Third party delivery channels working on behalf of government may wish to provide their own registration services or use those provided by a different third party.

### *2.2.3 Use of commercial technologies*

Government will make use of normal commercial technologies and techniques for registration and authentication.

---

[14] See section 2.3 for a definition of enrolment.

The use of system components that have been formally certified under the ITSEC and/or Common Criteria schemes is encouraged. However, there will be no general requirement for systems to undergo ITSEC or Common Criteria evaluations. The process for assurance of e-Government systems is described in the e-Government assurance framework.

It is considered acceptable to require a client to install a standard commercial security product in order to access e-Government services, for example a web browser with an up-to-date version of the Secure Sockets Layer (SSL) protocol. However, the requirement of client-installed custom software to access e-Government services should be avoided.

Government will make best efforts to ensure that services are accessible from a wide range of platforms (*eg* Personal Computers (PCs), kiosks *etc*), but cannot guarantee to include all. In those circumstances electronic services may be unavailable.

## 2.3 Trust models and current policy

A client must possess a certain degree of trust specified by the service provider in order to engage in an e-Government transaction.

Government needs to establish different levels of trust in the identity (both real-world and electronic) of clients wishing to use an e-Government service. Trust is acquired during the registration, authentication and enrolment stages.

Enrolment[15] is the process by which a client obtains authorisation[16] for a specific e-Government service. The authenticated electronic identity is then recorded as having authority to engage in relevant transactions. Enrolment may also entail registration of additional information relevant to the service in question. If appropriate, asserted information may be checked against available records. A client is only required to enrol once for each service and may only use those services for which he/she/it is enrolled. Requirements for enrolment need to be set on a service-by-service basis, in conjunction with relying parties.

As an example, there are a number of ways in which a service provider may obtain confidence in a real-world identity asserted[17] by a client to a level appropriate for a particular transaction. Two illustrative trust models are given below where trust in a real-world identity needs to be established:

a) A client registers with a trust service / Registration Authority (RA) and is issued with a credential after examination of relevant documentation. Evidence of real-world identity is securely embedded in the credential, or accessible securely *via* a look-up database or equivalent. The registration process thus establishes trust in the real-world identity of the client. This may be augmented during enrolment if further trust or additional client information is required for service delivery.

b) A client registers with an RA and is issued with a credential. The credential either does not contain or point to any information on real-world identity or the information is not releasable (*eg* privacy constraints prevent the release of relevant information for use other than for its original purpose). In this case, no trust is established in the real-world identity; trust would be obtained during enrolment or built up through a history of successful transactions.

---

15 The latest version of *e-Government strategy: security architecture.* Available at http://www.e-envoy.gov.uk

16 Defined in this document set as *the granting of rights to access services, information and resources.*

17 Not all services require a real-world identity. This is discussed further in section 2.5.

In each case, the level of trust from authentication (*ie* trust in an asserted electronic identity) relates directly to the type of credential used. Trust in a real-world identity can be obtained in both registration and enrolment.

At the current stage of development, the content and releasability of trusted information available directly or indirectly from a credential are not clear. Government is working towards clarifying this. While the government would prefer to use the trust model at a) above, this is not possible in the short term. The government currently thus uses the trust model at b).

## 2.4 General approach to registration and authentication

For the purposes of e-Government transactions, this document defines levels of registration and authentication that are appropriate for the different classes of transactions. In general, informal or lower value transactions will attract the lower levels of registration and authentication. Higher value or legally significant transactions will attract more stringent registration and authentication requirements.

It should be noted that, for a given transaction, registration and authentication might not possess equal emphasis and thus would attract different levels (*ie* level 1 registration does not necessarily imply a requirement for level 1 authentication and so on). As an example, a transaction such as pseudonymous access to medical testing would need unequal levels of registration and authentication since a real-world identity is not required but strong authentication is needed to ensure that the results are disclosed only to the client possessing the correct electronic identity.

Departments should allocate each electronic service to both a registration and authentication level in accordance with the guidance contained in this framework.

For each registration level, government defines a profile (set of requirements) setting out the mechanism for achieving the required degree of confidence in the real-world identity (which could be in the form of a particular role rather than a personal identity) and authority of the client. Separate profiles will be defined for business and citizen.

Similarly, profiles for authentication levels are being defined to set out the mechanisms for achieving the correct degree of confidence in the electronic identity of the client.

It is recognised that a Public Key Infrastructure (PKI), certificate-enabled applications or access tokens (such as smart cards) may not be available in the first instance. In this case, other mechanisms may be implemented initially, with an intention to adopt PKI mechanisms in due course.

## 2.5 Identification

When allocating registration and authentication levels to a transaction, e-Government service providers need to determine how much they need to know about the real-world identity of the client. There are broadly four categories of real-world identification; these are given below with their implied registration and authentication levels[18]:

a) Anonymous or pseudonymous: Neither the real-world identity of the client nor an electronic identity in an associated credential is required to complete the transaction. In the latter case, the client provides a pseudonym (registration level: 0, authentication level: 0).

[18] Registration levels are defined in section 3 and authentication levels in section 4.

b) Anonymous or pseudonymous with electronic identity[19]: The real-world identity of the client is not required to complete the transaction, but the electronic identity enables the service provider to recognise the client in repeat transactions (registration level: 0, authentication level: 1, 2 or 3).

c) Anonymous or pseudonymous with electronic identity and traceable: The real-world identity of the client is not required to complete the transaction, but the electronic identity enables the service provider to recognise the client in repeat transactions and could be used to retrieve the real-world identity *via* the RA, if required (registration level: 1, 2 or 3, authentication level: 1, 2 or 3).

d) Real-world identity established – the real-world identity of the client needs to be established to some degree of confidence before the transaction can be performed (registration level: 1, 2 or 3, authentication level: 1, 2 or 3).

As a rule, service provision should operate on a principle of maximum anonymity consistent with necessary functionality.

The table below sets out the likely combinations of registration and authentication levels that will be assigned to transactions. For example, there would seem to be little point for a transaction to need level 3 registration (extensive verification of real-world identity) and level 0 authentication (essentially unrestricted electronic access). Further guidance on the relationship between levels and assignment of a consistent set can be found in the overarching security framework.

An additional consideration is the use of delegate accounts whereby an individual is given delegated authority to undertake actions on behalf of an individual or organisation.

| | | Authentication level | | | |
|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 |
| Registration level | 0 | ✓ | ✓ | ✓ | ✓ |
| | 1 | ✗ | ✓ | ✓ | ✓ |
| | 2 | ✗ | ✗ | ✓ | ✓ |
| | 3 | ✗ | ✗ | ✗ | ✓ |

✗ unlikely combination

✓ likely combination

## 2.6 Other registration and authentication issues

*Delegate accounts*
When establishing the registration and authentication levels, consideration needs to be given to the use of delegate accounts whereby an individual is given delegated authority to undertake actions on behalf of an individual or organisation. Examples are establishing and using a power of attorney or giving a group of individuals 'signing' responsibility for placing orders.

A particular issue is whether it is necessary to identify an individual carrying out an e-business transaction on behalf of an organisation. The actual approach depends on the underlying business

[19] 'Anonymous with an electronic identity' and 'pseudonymous' are similar. The difference is that in the latter case, the electronic identity could be used to recognise the client in a subsequent transaction, while in the former case; there is no guarantee that the selected pseudonym is suitable as an electronic identity.

process being supported. For example, it might be appropriate for a purchase order to be placed by an identified organisation, with the identity of the individual being managed by the organisation. Similarly, for many transactions with central or local government, all that is of concern to the citizen is that a transaction is with an identified organisation.

# 3. Registration levels in government transactions

## 3.1 Introduction

This section defines the four registration levels, which represent degrees of confidence in an asserted real-world identity. The levels are layered according to the severity of consequences that might arise from misappropriation of a client's real-world identity. The more severe the likely consequences, the more confidence in an asserted real-world identity will be required to engage in a transaction.

Service provision guidelines relating to service control objective OS2 ('Effective user registration') are provided for each level. These comprise examples of physical supporting evidence, which might be required of an *individual undertaking face-to-face registration on his/her own account.* These examples are by no means intended to be definitive or exhaustive. Other guidelines are applicable to registration of organisations and their representatives, and remote registration, including online presentation of supporting evidence. For detailed service provision guidance, the reader is referred to government guidelines[20].

In allocating transactions to registration levels, the service provider must consider all the direct and indirect consequences laid out in the definitions of the levels (which include financial issues, personal safety, issues relating to the privacy of personal and commercial data and data protection legislation (see section 6)). In addition, departments will need to consider the terms 'minor', 'significant' and 'substantial' in the context of the parties likely to be affected. A significant financial loss to an individual might, for example, be a minor matter to a large company.

Departments must determine the level implied for each consequence and allocate the highest of these to the transaction. For example, if misappropriation of a client's real-world identity might result in risk to the client's personal safety, then the transaction must be allocated to registration level 3, even if potential financial loss or other consequences are minimal.

Service providers must consider the level assigned in terms of risks to the service as a whole, cost of implementation, practicality and overall business benefit. They may, in exceptional circumstances, be granted a waiver on adherence to this framework, subject to review during the assurance process.

Authentication of all types of client will consist of the presentation and checking of credentials. Registration to obtain these credentials will follow different guidelines for different types of client. Government has set out guidelines for registration of individuals[21] and organisations[22] to the degrees of confidence represented by the registration levels.

---

20 See www.e-envoy.gov.uk.

21 The latest version of *e-Government strategy framework policy and guidelines: HMG's minimum requirements for the verification of identity of individuals.* Available at http://www.e-envoy.gov.uk

It should be noted that if a credential has been issued at a particular registration level, then it can also be used for services that require a lower level of registration. For example, if a credential has been issued following registration at level 3, it may also be used in transactions requiring registration levels 2, 1 and 0.

The registration levels broadly represent degrees of certainty in an asserted real-world identity. However, the service provision guidelines given here should not be assumed to provide sufficient or acceptable evidence in a legal sense. The onus is on the business sponsor for a service to ensure that registration processes are adequate and legally binding where necessary.

## 3.2 Level 0 – minimal damage

### *3.2.1 Definition*

Level 0 registration is appropriate for e-Government transactions in which **minimal damage** might arise from misappropriation of real-world identity. In particular, misappropriation of a client's real-world identity at level 0 might result in at most:

minimal inconvenience to any party; or

no risk to any party's personal safety; or

no release of personally or commercially sensitive data to third parties; or

minimal financial loss[23] to any party; or

no damage to any party's standing or reputation; or

no distress being caused to any party; or

no assistance in the commission of or hindrance to the detection of serious crime.

### *3.2.2 Examples*

Examples of transactions that might merit level 0 registration include:

a) A client reads or downloads publicly available information from a government website. Access to this information does not require the client to reveal a real-world identity.

b) All other anonymous and pseudonymous transactions (except those that are categorised as traceable).

### *3.2.3 Service provision*

*OS2: Effective user registration*

No formal registration processes required, but might require issue of credentials.

---

22 The latest version of *e-Government strategy framework policy and guidelines: HMG's minimum requirements for the verification of identity of organisations.* Available at http://www.e-envoy.gov.uk

23 In this context, 'financial loss' includes the results of any claim for damages.

## 3.3 Level 1 – minor damage

### *3.3.1 Definition*

Level 1 registration is appropriate for e-Government transactions in which **minor damage** might arise from misappropriation of real-world identity. In particular, misappropriation of a client's real-world identity at level 1 might result in at most:

minor inconvenience to any party; or

no risk to any party's personal safety; or

no release of personally or commercially sensitive data to third parties; or

minor financial loss to any party; or

minor damage to any party's standing or reputation; or

minor distress being caused to any party; or

no assistance in the commission of or hindrance to the detection of serious crime.

### *3.3.2 Examples*

Examples of transactions that might merit level 1 registration include:

a) A client requests specific information (*eg* social security benefits) over the Internet and uses the credential to provide the delivery address. Misappropriation of a client's real-world identity would cause minimal inconvenience to the real identity holder.

b) A client arranges a meeting with a government official over the Internet. The credential provides basic assurance as to the validity of the real-world identity claimed, if such information is securely embedded in the credential or available to look up.

### *3.3.3 Service provision*

*OS2: Effective user registration*

Registration at this level is designed to prevent possible inconvenience to clients and deter casual false or misappropriated real-world identities.

For face-to-face registration (see section 3.1), the registrant is required to give a personal statement, which includes his/her full name, date and place of birth and current permanent address. At least one piece of reputable documentary evidence (*eg* passport) or third party corroboration (from a trustworthy source such as a bank or government department) is required in support.

## 3.4 Level 2 – significant damage

### *3.4.1 Definition*

Level 2 registration is appropriate for e-Government transactions in which **significant damage** might arise from misappropriation of real-world identity. In particular, misappropriation of a client's real-world identity at level 2 might result in at most:

significant inconvenience to any party; or

no risk to any party's personal safety; or

the release of personally or commercially sensitive data to third parties; or

significant financial loss to any party; or

significant damage to any party's standing or reputation; or

significant distress being caused to any party; or

assistance in the commission of or hindrance to the detection of serious crime.

### *3.4.2 Examples*

Examples of transactions that might merit level 2 registration include:

a) A client completes a tax return online. There must be substantial confidence in real-world identity since the return is legally binding. The return should not be open to forgery, and details of the income tax assessment should not be released to an unauthorised third party.

b) A client registers for council tax following a change of address. Since there are legal consequences for non-payment, substantial confidence in the client's real-world identity is required.

### *3.4.3 Service provision*

*OS2: Effective user registration*

Personal statement as for level 1, including information that may be crosschecked against supplied documentary/third party evidence.

In support are required one piece of documentary evidence that contains the registrant's signature and photograph (ideally a passport or National Identity Document) and one piece of evidence of activity in the community, such as a bank statement (two if the evidence of personal identity does not contain a photograph and signature). An item of third party corroboration may be substituted for one of the above pieces of evidence.

## 3.5 Level 3 – substantial damage

### *3.5.1 Definition*

Level 3 registration is appropriate for e-Government transactions in which **substantial damage** might arise from misappropriation of real-world identity. In particular, misappropriation of a client's real-world identity at level 3 might result in at most:

substantial inconvenience to any party; or

risk to any party's personal safety; or

the release of personally or commercially sensitive data to third parties; or

substantial financial loss to any party; or

substantial damage to any party's standing or reputation; or

substantial distress being caused to any party; or

assistance in the commission of or hindrance to the detection of serious crime.

### 3.5.2 Examples

Examples of transactions that might merit level 3 registration include:

a) A client wishes to register a change of address. This may involve a number of government systems that have existing information on the client. Strong registration is required since address is a primary attribute to be checked in the verification of real-world identity. An unauthorised change of address may entail serious consequences, such as misuse of real-world identity.

b) A client wishes to apply for a driving licence online. Again registration requirements are stringent since this is an accepted item of ID.

### 3.5.3 Service provision

*OS2: Effective user registration*

Personal statement is required as for level 2.

In support are required at least one piece of documentary evidence of personal identity, two of activity in the community and third party corroboration of information asserted in the registrant's personal statement.

# 4. Authentication levels in government transactions

## 4.1 Introduction

This section defines the four authentication levels, which represent degrees of confidence in an electronic identity presented to a service provider by means of a credential.

The levels are layered according to the degrees of severity of consequences that might arise from misappropriation of client's electronic identity / credentials. The more severe the likely consequences, the more confidence in an asserted electronic identity will be required to engage in a transaction.

In allocating transactions to authentication levels, the relying party must consider all the direct and indirect consequences laid out in the definitions of the levels. In addition, departments will need to consider the terms 'minor', 'significant' and 'substantial' in the context of the parties likely to be affected.

Departments must determine the level implied for each consequence and allocate the highest of these to the transaction. For example, if misappropriation of a client's electronic identity / credentials might result in risk to the client's personal safety, then the transaction must be allocated to authentication level 3, even if potential financial loss or other consequences are minimal.

Service providers must also consider the level assigned in terms of risks to the service as a whole, cost of implementation, practicality and overall business benefit. Departments may, in exceptional circumstances, be granted a waiver on adherence to this framework, subject to review during the assurance process.

Examples of transactions that might merit particular authentication levels are not intended to be taken as definitive.

Service provision guidelines are given in association with each level. These are related to service control objectives OS1 ('Effective user identification and authentication'), OS3[24] ('Effective access control') and OS4[25] ('Effective user access management').

The service control objectives OS3 and OS4 are discussed in more depth in the overarching security framework document. In addition to the service provision guidelines given here, service providers will need to consider the type of access (read / write and so on) appropriate to the client, transaction and level. These factors must also be considered for government users.

---

[24] Defined as: *"Access granted to e-Government service applications and assets is the minimum necessary for the identified user to obtain the service required"*.

[25] Defined as: *"Service authorities exercise complete control over the access rights granted to e-Government service users"*.

It should be noted that if a client holds a credential that is acceptable at a particular authentication level then it can also be used for all lower authentication levels. For example, if a credential is valid for authentication at level 3 (*ie* a digital certificate), it may also be used for authentication in transactions requiring authentication levels 2, 1 and 0.

## 4.2 Level 0 – minimal damage

### *4.2.1 Definition*

Level 0 authentication is appropriate for e-Government transactions in which **minimal damage** might arise from misappropriation of electronic identity, or no electronic identity is asserted. In particular, misappropriation of a client's credentials/electronic identity at level 0 might result in at most:

minimal inconvenience to any party; or

no risk to any party's personal safety; or

no release of personally or commercially sensitive data to third parties; or

minimal financial loss to any party; or

no damage to any party's standing or reputation; or

no distress being caused to any party; or

no assistance in the commission of or hindrance to the detection of serious crime.

### *4.2.2 Examples*

Examples of transactions that might merit level 0 authentication include:

a) A client reads or downloads publicly available information from a government website. Misappropriation of a client's credentials might cause minimal inconvenience to the client and no risk to safety or other adverse effects.

b) A client emails a government department with a request for general information and expects the material to be returned *via* email. Misappropriation of credentials might result in minimal inconvenience but no distress, damage to reputation or other consequences.

### *4.2.3 Service provision*

An authentication service is categorised as level 0 if no trust is put in the electronic identities asserted by the transacting parties, other than a presumption of correct operation of the underlying technology, or no electronic identity is asserted.

*OS1: Effective user identification and authentication*
No authentication is required.

*OS3: Effective access control*
Access will only be permitted to publicly available information.

*OS4: Effective user access management*
No management of client access is required, beyond overall technological limits on access.

Systems should be designed to prevent unauthorised access to username/password databases.

## 4.3 Level 1 – minor damage

### *4.3.1 Definition*

Level 1 authentication is appropriate for e-Government transactions in which **minor damage** might arise from misappropriation of electronic identity In particular, misappropriation of a client's credentials/electronic identity at level 1 might result in at most:

minor inconvenience to any party; or

no risk to any party's personal safety; or

no release of personally or commercially sensitive data to third parties; or

minor financial loss to any party; or

minor damage to any party's standing or reputation; or

minor distress being caused to any party; or

no assistance in the commission of or hindrance to the detection of serious crime.

### *4.3.2 Examples*

Examples of transactions that might merit level 1 authentication include:

a) A client apparently orders a low cost government publication over the Internet, but subsequently denies having done this. The impact is inconvenience and possible minor financial loss to the relying party, but there is no lasting impact on either party.

b) A client engages in online learning. There is need for authentication such that the client is recognised by the service and connected to the appropriate place in the course or given relevant assignment grades.

#### *Service provision*

*OS1: Effective user identification and authentication*

Clients will authenticate themselves to the system by the presentation of a credential, which, at this level, can be a username. Clients will demonstrate their right to that credential by presenting additional (non-public) information (for example, a password) or biometric measure(s). The system will authenticate users based on the validity of this credential/private information combination.

*OS3: Effective access control*

Access is only permitted to publicly available information and information pertaining to the client that has been collected in transactions up to level 1 for which the client is enrolled, subject to the principles of the Data Protection Act and the permitted use of the credential.

*OS4: Effective user access management*

Mechanisms should be implemented to time-limit access to transactions based on a specific item of knowledge. For example, management of client access should ensure that passwords are periodically changed, and that client accounts are disabled after a defined period of disuse and/or after a specific date.

Systems should be designed to prevent unauthorised access to username/password databases.

## 4.4 Level 2 – significant damage

### *4.4.1 Definition*

Level 2 authentication is appropriate for e-Government transactions in which **significant damage** might arise from misappropriation of electronic identity. In particular, misappropriation of a client's credentials/electronic identity at level 2 might result in at most:

significant inconvenience to any party; or

no risk to any party's personal safety; or

the release of personally or commercially sensitive data to third parties; or

significant financial loss to any party; or

significant damage to any party's standing or reputation; or

significant distress being caused to any party; or

assistance in the commission of or hindrance to the detection of serious crime.

### *4.4.2 Examples*

Examples of transactions that might merit level 2 authentication include:

a) A client files an income tax return electronically. Misappropriation of credentials might lead to the release of sensitive information to an unauthorised third party and possible significant financial loss and inconvenience[26].

b) A client specifies a bank account to be used for receipt of a significant refund. Misappropriation of credentials might cause significant financial loss to the client.

### *4.4.3 Service provision*

*OS1: Effective user identification and authentication*

Clients will authenticate themselves to the system by the presentation of a credential (which will preferably be a digital certificate). Clients will demonstrate their right to that credential through the use of, in the case of digital certificates, a private key and using a password or biometric measure. The system will authenticate users based on validity of public key/private key pairs, and on the validity of the credential and supporting information.

Use of a username/password at level 2 is strongly deprecated owing to the significant degradation of the security provided, and only acceptable while widespread public key infrastructures are unavailable. If use of a username/password is allowed at level 2, a timescale for conversion to PKI methods must be specified.

*OS3: Effective access control*

Access is only permitted to publicly available information and information pertaining to the client that has been collected in transactions up to level 2 for which the client is enrolled, subject to the principles of the Data Protection Act and the permitted use of the credential.

---

[26] Note that this is strictly an example and is not intended to be prescriptive. Misappropriation of credentials might also lead to fraudulent submission of a tax return and substantial inconvenience to the client (which would be level 3). Levels are to be assigned by the business sponsor in conjunction with the service provider and accreditor, on consideration of the entire business case.

*OS4: Effective user access management*
Validity of the credential must be time-bounded. In addition, the revocation status of the credential must be checked at the time of the transaction.

Systems should be designed to prevent unauthorised access to username/password databases.

## 4.5 Level 3 – substantial damage

### *4.5.1 Definition*
Level 3 authentication is appropriate for e-Government transactions in which **substantial damage** might arise from misappropriation of electronic identity. In particular, misappropriation of a client's credentials/electronic identity at level 3 might result in at most:

substantial inconvenience to any party; or

risk to any party's personal safety; or

the release of personally or commercially sensitive data to third parties; or

substantial financial loss to any party; or

substantial damage to any party's standing or reputation; or

substantial distress being caused to any party; or

assistance in the commission of or hindrance to the detection of serious crime.

### *4.5.2 Example*
An example of a transaction requiring level 3 authentication is a client wishing to collect their results after participating in an anonymous health-screening programme. There needs to be strong authentication such that the results are given to the citizen with the correct electronic identity. Disclosure of the results to the wrong citizen could result in unnecessary treatment for one client and an absence of treatment for another.

### *4.5.3 Service provision*
*OS1: Effective user identification and authentication*
Clients will authenticate themselves to the system by the presentation of a digital certificate. This will be held in an access token[27], which would ideally be a smart card, token or mobile device[28]. Clients will demonstrate their right to that credential through the use of a private key, and a password or biometric. The system will authenticate users based on the validity of public key/private key pairs, and on the validity of the credential.

Username/password combinations are not acceptable for level 3 authentication.

*OS3: Effective access control*
Access is permitted to publicly available information and information pertaining to the client that has been collected in transactions up to level 3 for which the client is enrolled, subject to the principles of the Data Protection Act and the permitted use of the credential.

---

27 In the short term, service providers may be granted a waiver on access tokens, subject to accreditor judgement.

28 As and when such devices are suitably secure.

*OS4: Effective user access management*
Validity of the credential must be time-bounded, and the revocation status of the credential must be checked at the time of the transaction.

Systems should be designed to prevent unauthorised access to databases containing correct client verification information.

## 4.6 Further guidance

More detailed guidance is available in the following documents:

a) e-Government guidelines on the use of passwords[29].

b) General *tScheme* documentation[30].

c) e-Government strategy security architecture[31].

[29] *e-Government strategy, guidelines on the use of passwords.* To be published.
[30] See http://www.tScheme.org.
[31] The latest version of *e-Government strategy: security architecture.* Available at http://www.e-envoy.gov.uk

# 5. Risks and countermeasures

## 5.1 Introduction

This section considers general risks pertaining to the registration and authentication processes and those pertaining to misappropriation of credentials/electronic identity and/or real-world identity.

It does not consider risks and countermeasures concerning information held within the government network domain or the trusted service provider domain (see the e-Government security policy framework[32]). Nor does it consider risks relating to specific technologies: technology-specific profiles will be needed to identify and counter specific risks to particular authentication technologies.

## 5.2 Description of risks and countermeasures

Possible countermeasures against each of the stated risks are set out below.

Where the main threat to the service is derived from the clients of the service, business units may need to determine the identity of an individual closer to the point of delivery of the service.

| Risk | Possible countermeasures |
|---|---|
| R1) Fictitious real-world identity<br>That a client will obtain a credential pertaining to a fictitious real-world identity. | Possible countermeasures to ensure that a real-world identity exists prior to the issue of credentials include:<br>C1a) checking the details given against population or organisation registers;<br>C1b) requiring that a trustworthy[33] person or organisation confirm the information given;<br>C1c) examining original documents. |
| R2) False details<br>That false information will be recorded against a genuine real-world identity, and subsequently given credence. | Possible measures to ensure that attributes submitted as part of the registration process are accurate include:<br>C2a) checking the details given against population or organisation registers;<br>C2b) requiring the registrant to certify the accuracy of the information given;<br>C2c) requiring that a trustworthy person or organisation confirm the information given. |

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

[33] In addition, there should be verification of the real-world identity of the trustworthy person or organisation.

| Risk | Possible countermeasures |
|---|---|
| R3) Theft of access token<br><br>That an access token containing a credential will be stolen from or while in transit to the user, and will either itself be used by an impostor or will be used to obtain information about a user for subsequent misuse. | Possible measures to reduce the risk of theft include:<br><br>C3a) requiring that access tokens are delivered using appropriate postal or courier services or issued in person only to the registered user;<br><br>C3b) ensuring that access tokens are usable only in conjunction with a PIN, password, biometric or other user verification mechanism. Any secret data intended for use in the verification process shall be delivered or issued separately from the token itself or stored securely within the token;<br><br>C3c) ensuring that the minimum of public data is contained in accessible form on the token. |
| R4) Real-world identity theft<br><br>That a genuine real-world identity will be misappropriated at the time of registration. | Possible measures to ensure that credentials are issued only to the genuine holder of that real-world identity include:<br><br>C4a) examining original documents at the time of registration;<br><br>C4b) asking the registrant questions derived from unpublished information about the real-world identity holder;<br><br>C4c) requiring that a trustworthy person or organisation vouch for the registrant;<br><br>C4d) contacting the supposed registrant at their registered address or telephone number;<br><br>C4e) sending the credential only to the registered address of the real-world identity holder. |
| R5) Interception or revelation of secret authentication information<br><br>That secret information (such as a PIN or private signing key) will be intercepted in transmission when the credential is used, will be accessed by an e-Government user, or will be revealed deliberately or inadvertently by the client or another party. | Possible measures to reduce the risk of secret authentication information being intercepted or revealed include:<br><br>C5a) ensuring that secret information is not transmitted at all, for example, by using a smart card (for which the private key never leaves the token) to sign or encrypt information;<br><br>C5b) ensuring that secret information is transmitted only in encrypted form, or *via* an encrypted channel, or *via* an inherently secure communications link;<br><br>C5c) ensuring that secret information is not transmitted en bloc in clear; for example, in a call centre transaction the client may be asked to provide one character only from each of a series of secret numbers and/or phrases, and the operator should only have access to those single characters;<br><br>C5d) using dynamic rather than static information: in the case of verification of identity to a call centre, for example, asking the caller about a recent transaction is likely to be more reliable than asking about an account number or mother's maiden name, which may have been discovered by an impostor;<br><br>C5e) placing a contractual requirement on the client not to disclose secret authentication information. |
| R6) Retention of secret authentication information in an untrusted terminal<br><br>That secret information will be retained by an untrusted terminal (such as a home or office PC, PC in an Internet cafe or public kiosk). Such secret information may include for example private signing keys used to perform cryptographic functions within the terminal, and PIN numbers entered into a web-based form and subsequently held in cache. | Countermeasures against this risk will need to be technology-specific, but could include:<br><br>C6a) ensuring secrets are not stored in an untrusted environment, rather they are kept wholly in a trusted token such as a smart card programmed to perform the signing act ;<br><br>C6b) ensuring that secrets are properly controlled and positively purged when no longer required. |

| Risk | Possible countermeasures |
|---|---|
| R7) Unauthorised use of access token<br><br>That an access token will be used by a user other than the one issued with the token. | Measures to protect against unauthorised use of an access token include:<br><br>C7a) Requiring that authentication devices be protected by a system of correct user verification, such as a password, PIN or biometric. |
| R8) Use of compromised credential<br><br>That a credential will be used after it has been compromised. | Possible countermeasures against use of a compromised credential include:<br><br>C8a) enabling and encouraging clients and relying parties to report suspected compromise to a continually available helpdesk service;<br><br>C8b) limiting the life of credentials to a fixed term;<br><br>C8c) enabling relying parties to check the validity of a credential at time of use, by reference to a credential revocation list;<br><br>C8d) enabling relying parties to obtain positive verification of the validity of a credential at time of use, by means of an authorisation procedure. |
| R9) Use of credential after substantive change in circumstances<br><br>That a credential will be used when a change in circumstances means that the credential would not normally have been issued | Possible measures to protect against the use of a credential after a substantive change in circumstances include:<br><br>C9a) contractually obliging the client to notify any change in circumstances;<br><br>C9b) in the case of organisations, monitoring notifications of cessation of trading and stopping credentials;<br><br>C9c) requiring organisations to notify the RA when a credential issued to one of their staff for business purposes should be stopped. |
| R10) Use of credential for unintended purposes<br><br>That a credential will be used in connection with a transaction for which the issuer is not prepared to warrant it, because of the nature or value of the transaction. | Possible measures to reduce the risk of a credential being used for unintended purposes include:<br><br>C10a) credentials being issued against practice statements;<br><br>C10b) credentials such as digital certificates, and the tokens that contain them, incorporating limitations as to use;<br><br>C10c) where the main threat to the service is derived from the clients of the service, business units may need to determine the identity of an individual closer to the point of delivery of the service. |
| R11) Withdrawal of credential without due cause<br><br>That a credential will be withdrawn due to a false or malicious report of change in circumstances, compromise of credential, etc. | Possible measures to reduce the risk of, or inconvenience caused by, inappropriate withdrawal of a credential include:<br><br>C11a) the ability to suspend rather than revoke a credential;<br><br>C11b) a continuously-available helpdesk service for clients;<br><br>C11c) the ability to replace a credential rapidly after withdrawal and/or rescind the revocation;<br><br>C11d) registration authorities having access to verification information to provide at least some assurance that the person reporting compromise or change of circumstances is genuine. |

| Risk | Possible countermeasures |
|---|---|
| R12) Fraudulent use of credential<br><br>That a credential holder will attempt to use their credential, either personally or through a third party, for transactions to which they are not entitled. | Possible measures to reduce the risk of unwarranted use of a credential include:<br><br>C12a) contractually obliging the credential holder (client) to use the credential for its intended purpose;<br><br>C12b) using dynamic information to check that the credential is still held by the correct client;<br><br>C12c) using biometric data to ensure that the credential is held by the correct client;<br><br>C12d) requiring clients to register and enrol for each service before use;<br><br>C12e) ensuring that services provided are in accordance with limitations on use of the credential. |
| R13) Hacker attack<br><br>That a hostile outsider may gain direct access to e-Government services with the objective of achieving some personal gain, embarrassment to the UK, denying access to the system or causing damage to the system. | Possible measures to reduce the risk of compromise of services due to hacker attack include:<br><br>C13a) firewall deployment;<br><br>C13b) penetration testing;<br><br>C13c) IDS deployment;<br><br>C13d) maintaining the security patch state of the business' application and infrastructure software. |
| R14) Dispersed storage of information<br><br>That client information will be at greater risk of compromise due to fragmentation of information collected across various e-Government services. | Possible measures to reduce the risk of compromise of client information due to dispersed storage include:<br><br>C14a) appropriate design of services to minimise such duplication of information;<br><br>C14b) ensuring compliance with the Data Protection Act. |

# 6. Data protection

## 6.1 Data protection

There are potentially a number of data processors in any scheme that provides access to e-Government services. These include the RA, the relying party and any organisation verifying a client's real-world identity on behalf of the relying party at the time of transaction. All are bound by the requirements of the Data Protection Acts and by the data protection principles.

Data controllers must comply with the following eight data protection principles. These may be summarised as requiring that personal data shall be:

a) processed fairly and lawfully;

b) obtained and processed for specified and lawful purposes;

c) adequate, relevant and not excessive;

d) accurate and up to date;

e) held for no longer than necessary;

f) processed in accordance with subject rights;

g) kept secure; and

h) kept within the European Economic Area, unless there are adequate safeguards.

Where personal data is processed on behalf of a data controller by a third party, the activities of the data processor must be governed by a written contract. In addition, providers of registration services to government must comply with any applicable data protection and retention policy.

A number of specific points arise in respect of access to e-Government services. In particular:

a) in order to comply with the seventh principle, adequate registration, authentication and enrolment is required to prevent unauthorised disclosure of personal data: indeed, for a given government service, there is a substantial likelihood that the mechanism for the release of data in respect of that service will need to be stronger than that for submission of the data in the first place;

b) data obtained for the purpose of verifying real-world identity should not be used for secondary purposes;

c) there must be transparency: it should be clear to the data subject why registration or enrolment information is being requested;

d) whilst it may be necessary to retain for a reasonable period information given when real-world identity is verified, for example for reasons of accountability and audit, the requirements of the fifth principle must be considered; and

e) where a trust service provider registers a client on behalf of one or more relying parties (as in the case of a 'portal' service), that trust service provider must pass on to each of the relying parties only that information which is relevant.

# A. Abbreviations

| | |
|---|---|
| AEB | Alliance for Electronic Business |
| CA | Certification Authority |
| CRL | Certificate Revocation List |
| NI | National Insurance |
| PAYE | Pay As You Earn |
| PC | Personal Computer |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| RP | Relying Party |
| VAT | Value Added Tax |
| WAP | Wireless Access Protocol |

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