E-government strategy framework policy and guidelines:

Registration and authentication

v2.1

2 November 2001

Cover + 54 pages

List of contents

Document status and history

Issue No	Date of Issue	Issued by	Reason for issue
1.0	December 1999	IAGC	First publication
Draft	December 2000	Office of the eEnvoy	Second consultation
2.0	20 September 2001	Curtis+Cartwright Consulting Ltd	Modification to incorporate initial comments received from public consultation for review by the Office of the e-Envoy
2.1	2 November 2001	Curtis+Cartwright Consulting Ltd	Modification to include minor comments from Office of the e-Envoy prior to further public consultation

This page is intentionally blank

1 Introduction

1.1 Ownership and maintenance

1 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.

2 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.

3 This version of the document incorporates comments received after a public consultation on an earlier draft. It is intended for a further public consultation.

1.2 Terminology

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

a) **Registration**: This is the process by which a client 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) **Authentication**: The process by which the electronic identity[3] of a client 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 client 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.

5 A list of abbreviations is also provided at annex A. The meaning ascribed to these and other specific terms in the document is provided in the glossary at annex B.

---

1 *Modernising Government white paper*.

2 *Modernising government - framework for information age government – security*, V1.0, 2 November 2001.

3 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 client 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.

1.3 Who should read this document?

6 This document is aimed at those procuring and providing e-government services. This includes the Departments and non-departmental public sector bodies charged with the provision of e-government services, regulatory bodies responsible for the proper audit and control of public assets and information, and the suppliers and service providers who may provide and operate such systems on behalf of government.

1.4 Background

7 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.

8 Clients must also be able to identify the government systems and personnel with which they deal. Work on this aspect is under way but is outside the scope of this paper.

9 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[4] will need to be confident that a service is secure and that their privacy is being maintained.

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

1.5 Objective

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

---

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.

12 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[5].

1.6 Scope

13 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.

14 It is not applicable 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. In these circumstances, normal commercial practice should be applied.

1.7 Organisations affected by this document

15 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.

16 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.

17 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;

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

---

5 *E-government strategy: security architecture*, V1.3, 2 November 2001.

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.

18 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

19 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.

20 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.

21 The trust services framework document[6] addresses the following objectives:

a) OS5 – Non repudiation;
b) OS6 – Evidence of receipt;
c) OS7 – Trusted commitment service;
d) OS9 – Integrity.

22 The confidentiality framework document[7] addresses the following objective:

a) OS8 – Privacy and confidentiality.

23 The business services framework document[8] addresses the following objectives:

a) OS10 – Service availability;
b) OS11 – Information availability;
c) OS13 – Effective audit and accounting.

24 The network defence framework document[9] addresses the following objective:

a) OS12 – Service protection.

1.9 Availability of advice

25 In the first instance, advice on the application of the registration and authentication framework may be obtained from the Office of the e-Envoy[10].

---

6 *E-government strategy framework policy and guidelines, trust services,* V2.1, 2 November 2001.
7 *E-government strategy framework policy and guidelines, confidentiality,* V2.1, 2 November 2001.
8 *E-government strategy, framework policy and guidelines, business services,* V1.0, 2 November 2001.
9 *E-government strategy framework policy and guidelines, network defence,* V1.1, 2 November 2001.
10 http://www.e-envoy.gov.uk.

26 CESG[11] 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.

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

This page is intentionally blank

2 Summary of government's approach to registration and authentication

2.1 Introduction

27 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.

28 An overarching operations concept for a client engaging in e-government transactions is given at annex C.

2.2 Third party participation in provision of e-government services

2.2.1 Provision of registration services by third parties

29 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, currently being developed 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.

30 Any third party providing registration services to support e-government transactions should normally be approved by a suitable UK government scheme such as *tScheme*.

2.2.2 Third party service delivery

31 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[12] of the clients they deal with 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

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

33 The use of ITSEC/Common Criteria - evaluated system components is encouraged. However, there will be no general requirement for such systems to undergo ITSEC

12 See section 2.3 for a definition of enrolment.

or Common Criteria evaluations. The process for assurance of e-government systems is described in the e-government assurance framework[13].

34 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 custom client-installed software to access e-government services should be avoided.

35 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

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

37 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.

38 Enrolment[14] is the process by which a client obtains authorisation for a specific online 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.

39 As an example, there are a number of ways in which a service provider may obtain confidence in a real-world identity asserted[15] 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.

---

13 *E-government strategy framework policy and guidelines, assurance,* discussion draft 0.C.

14 *E-government strategy: security architecture,* V1.3, 2 November 2001.

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

40 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.

41 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 paragraph 39a), this is not possible in the short term. The government currently thus uses the trust model at paragraph 39b).

2.4 General approach to registration and authentication

42 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.

43 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.

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

45 For each registration level, government is defining 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.

46 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.

47 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

48 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[16]:

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).

b) Anonymous or pseudonymous with electronic identity[17]: 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).

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

50 The following table 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 and level 0 authentication.

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

✗ unlikely combination

✓ likely combination

16 Registration levels are defined in section 3 and authentication levels in section 4.

17 '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.

3 Registration levels in government transactions

3.1 Introduction

51 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.

52 Service provision guidelines relating to service control objective OS2 ('Effective user registration') are provided for each level. These comprise examples of 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 (and are not applicable to registration of organisations, their representatives, and remote registration). For detailed service provision guidance, the reader is referred to government guidelines, which are summarised at annex D.

53 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.

54 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.

55 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. Departments may, in exceptional circumstances, be granted a waiver on adherence to this framework, subject to review during the assurance process.

56 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 and organisations[18] to the degrees of confidence represented by the registration levels.

57 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.

---

18 No current references to these documents are available. The guidelines summarised at annex D reflect the current situation, but are under going revision and discussion. They will be issued on the Office of the eEnvoy website when they are available.

3.2 Level 0 – no confidence

3.2.1 Definition

58 **No confidence** is placed in the asserted real-world identity of the client or no real-world identity is asserted. In particular, misappropriation of a client's real-world identity at level 0 might result in at most:

- minimal inconvenience to the client; or
- no risk to the client's personal safety; or
- no release of personal or commercially sensitive data to third parties; or
- minimal financial loss[19] 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

59 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

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

3.3 Level 1 – balance of probabilities

3.3.1 Definition

61 On the **balance of probabilities**, the registrant's real-world identity is verified. In particular, misappropriation of a client's real-world identity at level 1 might result in at most:

- minor inconvenience to the client; or
- no risk to the client'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.

---

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

3.3.2 Examples

62 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.

3.3.3 Service provision

OS2: Effective user registration

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

64 For face-to-face registration (see paragraph 52), the registrant is required to give a personal statement, which includes his/her full name, date 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 – substantial assurance

3.4.1 Definition

65 There is **substantial assurance** that the registrant's real-world identity is verified. In particular, misappropriation of a client's real-world identity at level 2 might result in at most:

- significant inconvenience to the client; or
- no risk to the client's personal safety; or
- the release of personal 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

66 Examples of transactions that might merit level 2 registration include:

a) A client completes a tax return online. There must be substantial assurance of 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 assurance of the client's real-world identity is required.

3.4.3 Service provision

OS2: Effective user registration

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

68 In support are required one piece of documentary evidence that contains the registrant's signature and photograph (*eg* passport) 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 photo and signature).

3.5 Level 3 – beyond reasonable doubt

3.5.1 Definition

69 The registrant's real-world identity is verified **beyond reasonable doubt**. In particular, misappropriation of a client's real-world identity at level 3 might result in at most:

- substantial inconvenience to the client; or
- risk to the client's personal safety; or
- the release of personal 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

70 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 identity.

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

3.5.3 Service provision

OS2: Effective user registration

71 Personal statement is required as for level 2.

72 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.

This page is intentionally blank

4 Authentication levels in government transactions

4.1 Introduction

73 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.

74 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.

75 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.

76 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.

77 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.

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

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

80 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 – no confidence

4.2.1 Definition

81 **No confidence** is placed in the asserted electronic identity of the client 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 the client; or

- no risk to the client's personal safety; or
- no release of personal 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

82 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

83 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

84 No authentication is required.

OS3: Effective access control

85 Access will only be permitted to publicly available information.

OS4: Effective user access management

86 No management of client access is required, beyond overall technological limits on access.

4.3 Level 1 – balance of probabilities

4.3.1 Definition

87 Level 1 authentication is appropriate for e-government transactions in which it is sufficient that on the **balance of probabilities** the relying party may have confidence in an asserted electronic identity. In particular, misappropriation of a client's credentials/electronic identity at level 1 might result in at most:

- minor inconvenience to the client; or
- no risk to the client'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

88 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.

4.3.3 Service provision

OS1: Effective user identification and authentication

89 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

90 Access will only be allowed to non-sensitive data pertaining to the authenticated client, and to publicly available information.

OS4: Effective user access management

91 Mechanisms should be implemented to time-limit access to transactions based on a specific item of knowledge.

92 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.

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

4.4 Level 2 – substantial assurance

4.4.1 Definition

94 Level 2 authentication is appropriate for e-government transactions between parties that are of an official nature, in which there is a need for **substantial assurance** in an

asserted electronic identity. In particular, misappropriation of a client's credentials/electronic identity at level 2 might result in at most:

- significant inconvenience to the client; or
- no risk to the client's personal safety; or
- the release of personal 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

95 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.

4.4.3 Service provision

OS1: Effective user identification and authentication

96 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.

97 Use of a username/password at level 2 is deprecated, but acceptable while widespread public key infrastructures are unavailable.

OS3: Effective access control

98 Access is only permitted to publicly available information and information pertaining to the client that has been collected in transactions up to level 2. Such access must also be governed by the permitted use of the credential.

OS4: Effective user access management

99 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.

4.5 Level 3 – beyond reasonable doubt

4.5.1 Definition

100 Level 3 authentication is appropriate for e-government transactions of an official nature. In order to engage in these transactions an asserted electronic identity must be verified **beyond reasonable doubt**. In particular, misappropriation of a client's credentials/electronic identity at level 3 might result in at most:

- substantial inconvenience to the client; or
- risk to the client's personal safety; or
- the release of personal 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 Examples

101 Examples of transactions requiring level 3 authentication include:

a) A client wishes 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

102 Clients will authenticate themselves to the system by the presentation of a digital certificate. This will preferably be held in an access token, which would ideally be a smart card, token or mobile device. 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.

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

OS3: Effective access control

104 Access is permitted to all information pertaining to the authenticated client involved in services up to and including level 3 for which the client is enrolled, subject to the principles of the data protection act.

OS4: Effective user access management

105 Validity of the credential must be time-bounded, and the revocation status of the credential must be checked at the time of the transaction.

4.6 Further guidance

106 More detailed guidance is available in the following documents:

a) e-government guidelines on the use of passwords[20].

b) General *tScheme* documentation[21].

c) e-government strategy security architecture[22].

20 *E-government strategy, guidelines on the use of passwords.* To be published.

21 See http://www.tScheme.org.

22 *E-government strategy: security architecture*, V1.3, 2 November 2001.

5 Risks and countermeasures

5.1 Introduction

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

108 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). 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

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

110 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 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: C1a) checking the details given against population or organisation registers; and/or C1b) examining original documents.
R2) False details 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: C2a) checking the details given against population or organisation registers; and/or C2b) requiring the registrant to certify the accuracy of the information given; and/or C2c) requiring that a trustworthy person or organisation confirm the information given.
R3) Theft of access token That an access token containing a credential will be stolen from or while in transit to the client, and will either itself be used by an impostor or will be used to obtain information about a client for subsequent misuse.	Possible measures to reduce the risk of theft include: C3a) requiring that access tokens are delivered using appropriate postal or courier services or issued in person only to the registered client; and/or 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; and/or C3c) ensuring that the minimum of public data is contained in accessible form on the token.

Risk	Possible countermeasures
R4) Real-world identity theft 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: C4a) examining original documents at the time of registration; and/or C4b) asking the registrant questions derived from unpublished information about the real-world identity holder; and/or C4c) requiring that a trustworthy person or organisation vouch for the registrant; and/or C4d) contacting the supposed registrant at their registered address or telephone number; and/or C4e) sending the credential only to the registered address of the real-world identity holder.
R5) Interception or revelation of secret authentication information 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 a member of the relying party's staff, 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: C5a) ensuring that secret information is not transmitted at all, for example, by using a smart card to sign or encrypt information; or C5b) ensuring that secret information is transmitted only in encrypted form, or *via* an encrypted channel, or *via* an inherently secure communications link; and/or 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; and/or C5d) using dynamic rather than static information: in the case of authentication 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; and/or C5e) placing a contractual requirement on the client not to disclose secret authentication information.
R6) Retention of secret authentication information in an untrusted terminal 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: 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 or C6b) ensuring that secrets are properly controlled and positively purged when no longer required.
R7) Unauthorised use of access token That an access token will be used by a client other than the one issued with the token.	Measures to protect against unauthorised use of an access token include: C7a) Requiring that authentication devices be protected by a system of correct client verification, such as a password, PIN or biometric.

5 Risks and countermeasures

Risk	Possible countermeasures
R8) Use of compromised credential That a credential will be used after it has been compromised.	Possible countermeasures against use of a compromised credential include: C8a) enabling and encouraging clients and relying parties to report suspected compromise to a continually available helpdesk service; and C8b) limiting the life of credentials to a fixed term; and C8c) enabling relying parties to check the validity of a credential at time of use, by reference to a credential revocation list; and 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 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: C9a) contractually obliging the client to notify any change in circumstances; and C9b) in the case of organisations, monitoring notifications of cessation of trading and stopping credentials; and 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 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: C10a) credentials being issued against practice statements; and C10b) credentials such as digital certificates incorporating limitations as to use; and 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 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: C11a) the ability to suspend rather than revoke a credential; and C11b) a continuously-available helpdesk service for clients; and C11c) the ability to replace a credential rapidly after withdrawal; and 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.
R12) Fraudulent use of credential 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: C12a) contractually obliging the credential holder (client) to use the credential for its intended purpose; and C12b) using dynamic information to check that the credential is still held by the correct client; and C12c) using biometric data to ensure that the credential is held by the correct client; and C12d) ensuring that services provided are in accordance with limitations on use of the credential.

Risk	Possible countermeasures
R13) Hacker attack 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: C13a) firewall deployment; and C13b) penetration testing; and C13c) maintaining the security patch state of the business' application and infrastructure software.

6 Data protection

6.1 Data protection

111 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.

112 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.

113 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 the stated data protection and retention policy[23].

114 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;

23 Annex C of Channels for Electronic Service Delivery: Draft Operating Policy, published by the Office of the e-Envoy.

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	Credential 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

This page is intentionally blank

B Glossary

1 The following definitions align with those set out in related security framework documents.

B.1.1 Access token

2 An access token is some medium that contains a credential, for example a smartcard that contains a digital certificate.

B.1.2 Anonymous client

3 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.1.3 Assurance

4 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.1.4 Authentication

5 Authentication is the process by which the electronic identity of a client 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 client 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.1.5 Authorisation

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

B.1.6 Government back office system

7 A government back office system is the computer system within a government department, agency, local or regional authority, which completes a requested service based on data passed from the government gateway.

B.1.7 Certificate Revocation List (CRL)

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

B.1.8 Certification Authority (CA)

9 A certification authority issues, manages and revokes credentials at the request of Registration Authorities.

B.1.9 Challenge response

10 Challenge response is a mechanism based on the use of PKI that is typically used to test whether the owner of a digital certificate can be authenticated for a particular service.

B.1.10 Client

11 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.1.11 Client registration

12 Client registration is the process by which a client first registers with the government gateway by presenting an acceptable credential. 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.

B.1.12 Credential

13 A credential is a set of information, which is used by a client 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. Credentials are issued to the client by or on the instructions of a registration authority.

B.1.13 Credential revocation list

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

B.1.14 Directory

15 A directory is the set of information that allows the government gateway 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.1.15 Electronic identity

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

B.1.16 Enrolment

17 Enrolment is the process by which a client obtains authorisation for a specific online 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 the client is enrolled. Requirements for enrolment need to be set on a service-by-service basis.

B.1.17 Government gateway

18 The government gateway 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.

19 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.

20 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.

B.1.18 Government gateway registration

21 Government gateway registration is the process in which the government gateway can establish a credential and present this to the client for authentication of the government gateway to the client.

B.1.19 Practice statement

22 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.1.20 Pseudonymous client

23 A pseudonymous client is one who chooses only to reveal a pseudonym as part of 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 pseudonymous and untraceable.

B.1.21 Real-world identity

24 A real-world identity is a set of attributes (*eg* name, date of birth, national insurance number), which uniquely discriminates between clients. A real-world identity may incorporate a particular role played by the client. Depending on the transaction, a client may be required to reveal the real-world identity or may be permitted to use a pseudonym or remain anonymous.

B.1.22 Registration

25 Registration is the process by which a client 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.1.23 Registration Authority

26 A Registration Authority (RA) is the organisation that validates evidence both of a client'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.1.24 Registrant

27 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.1.25 Registration and enrolment policy

28 It is envisaged that there would be a detailed registration and enrolment policy statement for the government gateway. 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 client registration and enrolment, the appeals process, acceptable credentials and the relationship between a credential provider and the government.

B.1.26 Relying Party

29 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.1.27 Roles

30 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.

B.1.28 Status responder

31 A status responder is an organisation (such as a Certification Authority), which checks the validity of the credential, and the client's right to use the credential, when a service is requested. The status responder is usually the credential issuer.

B.1.29 Trust service provider

32 Registration authorities are also referred to as trust service providers, since they provide a measure of trust in the asserted real-world identity of a client.

B.1.30 UKonline

33 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.1.31 UKonline citizen portal

34 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 government back office systems operated by government departments and agencies. The UKonline citizen portal will also present publicly available information.

35 The UKonline citizen portal is one of a number or portals that provide access to UKonline services.

B.1.32 UKonline service

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

B.1.33 Unenrolment

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

B.1.34 Unpublished data

38 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.

This page is intentionally blank

C Overarching concept of operations for access to e-government services

C.1 Introduction

39 This section provides a conceptual overarching concept of operations for a client accessing e-government services *via* the government gateway, though not all steps will be undertaken in all circumstances. Moreover, not all processes will be a government responsibility.

40 The concept of operations comprises the following processes that are described further below:

a) registration;
b) client registration and authentication;
c) enrolment;
d) service use;
e) government gateway registration and authentication;
f) unenrolment on completion of need for a specific enrolled service;
g) deregistration on completion of need for e-government services.

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

C.2 Registration

42 A client first decides that he or she wishes to make use of an egovernment service and then determines the necessary steps to gain access to the service. For those e-government services that need it, the client engages in the registration process with a RA. Successful registration leads to the issue of a credential (*eg* a client identifier and password or a digital certificate) by a credential issuer.

43 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 e-government service.

44 Examples of registration include:

a) obtaining a client identifier and password combination from a government department to use the e-government 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 use for access to e-government services; this service could be accessed *via*, for example, a PC, a Wireless Access Protocol (WAP) phone or in the future a kiosk.

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

46 The Certification Authority (CA) would also manage credentials to ensure that they were suspended or withdrawn, and where appropriate replaced, in the event of the client requesting it, the theft or compromise of the credential, the client's death, resignation, dismissal, change of name, cessation of trading or other significant

change of circumstances. The CA would maintain a list of credentials that had been revoked (referred to as a Credential Revocation List (CRL)).

47 It is envisaged that the RA and the CA would maintain a helpdesk service, which is available at all times, to enable the client/credential holder to notify suspected loss or compromise of credentials, change of circumstances, etc.

48 It is also envisaged, particularly in respect of business credentials, that the RA and CA would monitor information used to issue credentials and proactively suspend credentials in the event of change of circumstances (such as cessation of trading).

C.3 Client registration and authentication

49 After registration is completed and the appropriate credential issued, the client might decide to use an e-government service. For those e-government services that need it, the client first registers 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).

50 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.

51 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 back office services.

52 After successful client registration, the client may enrol for one or more e-government services.

53 On a subsequent visit, the client presents the credential, 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.

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

C.4 Enrolment

55 After successful registration with the government gateway, the client may enrol for one or more specific e-government 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 back office system, while others (*eg* on-line learning) may not.

56 Part of the enrolment process could 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 appropriate records, if any, held on a back

office system that correspond to the client (*eg* name, NI number, tax reference number etc for an Inland Revenue service).

57 The combination of registration, client registration, authentication and enrolment will enable appropriate trust to be built up in the client for access to the required e-government services.

58 The combination of client registration and enrolment will allow the government gateway to map uniquely between the client's credential and the corresponding information held on the back office system supporting the service requested by the client.

59 Once a client has enrolled for a specific service, the client may access that service.

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

C.5 Service use

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

62 The service application 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 undertake the relevant transaction.

63 The client might choose to have simultaneous sub-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.

64 Normally, the client would terminate each e-government sub-session and finally terminate the e-government session.

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

66 Service providers need to be aware of the possibility that clients may attempt to engage in transactions *via* inappropriate channels (*eg* in general emails to departments). A procedure needs to be implemented to ensure these types of transactions are dealt with and logged within a reasonable time from submission.

C.6 Government gateway registration and authentication

67 For high levels of trust, it might be necessary and appropriate for the government gateway to establish its identity to give assurance to the client that he or she is really accessing the government gateway. It is the government's vision that this will be

supported by use of a digital certificate bound to the relevant e-government service provider.

C.7 Unenrolment from a specific enrolled service

68 At some point, the client might decide that a specific e-government 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. If appropriate, the government gateway would also inform the relevant back office system.

C.8 Deregistration on completion of need for e-government services

69 At some point, the client might decide that no further e-government services were either required, or would otherwise cease to use e-government 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. If appropriate, the government gateway would also inform relevant back office systems.

C.9 Roles, intermediaries and delegate accounts

Multiple roles

70 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

71 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.

72 Mechanisms must be 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 back office systems.

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

C Overarching concept of operations for access to e-government services

74 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

75 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 credential 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.

76 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.

C.10 Registration and enrolment policy statement

77 It is envisaged that there would be a government 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 e-government service;

c) what information needs to be collected from a client during client registration and service enrolment for each e-government service;

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

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

This page is intentionally blank

D Summary of e-government registration guidelines

D.1 Introduction

78 The government has produced guidelines for the registration ('verification of identity') of individuals[24] and organisations[25]. This annex provides a summary of those guidelines for illustrative purposes. However, for definitive service provision information and guidance, the reader is referred to the original documents.

D.2 Registration of individuals

79 E-government service providers will follow the guidelines set out by the government for the registration of individuals. They are summarised here.

D.2.1 Definitions

80 In the context of the guidelines, identity means a set of attributes that together identify a natural person. This is interpreted here as a real-world identity.

81 To validate is to demonstrate that a claimed real-world identity exists (*ie* the attributes belong to a real person).

82 Verification is the process by which it is established that the registrant is who he/she claims to be.

D.2.2 Scope

83 These guidelines only cover those cases where individuals are registered on their own account. They also allow for registration of an individual by an agent or proxy.

D.2.3 Methods of registration

84 Registration may be face-to-face or remote. If remote, supporting evidence may be presented physically or remotely.

85 The type and variety of supporting evidence required for the validation and verification of real-world identity will vary between these methods of registration. In general, face-to-face registration will require less supporting evidence than remote registration.

D.2.4 Types of evidence

86 The kinds of evidence which may be used to validate and verify real-world identity fall into five main categories:

---

24 No current reference to this document is available – see footnote 18.

25 No current reference to this document is available – see footnote 18.

a) **Personal statement**. The registrant or his/her agent provides details on his/her real-world identity and history in order to uniquely distinguish the individual and to provide material that can be checked against other classes of evidence. This will most likely be in the form of a questionnaire. This may request attributes of the real-world identity such as:

   i) name;

   ii) date of birth;

   iii) permanent address (or contact address / care-of address);

   iv) educational history;

   v) marital history;

   vi) employment details.

b) **Documentary evidence**. In this context, this refers to documents in the possession of the registrant, which can confirm some of the attributes of the real-world identity referred to above. These fall into two main categories:

   i) Evidence of real-world identity *per se*. These will usually hold the registrants signature and preferably also photograph. Documents such as passport, birth certificate and national ID cards, for example, fall into this category.

   ii) Evidence of 'activity in the community'. This evidence provides corroboration for other information. These documents will as a rule be dated, bear the name and where possible address of the registrant and be from a trustworthy source. Bank statements and utility bills are examples of this kind of evidence.

   Where more than one document is sought, it is appropriate to seek at least one from each category.

c) **Third party corroboration**. This type of evidence comprises information from a trustworthy third party, obtained by direct contact or as published information. The registrant should **not** be directly involved, apart from to give consent. Trusted third parties may include organisations such as:

   i) government departments and agencies;

   ii) local authorities;

   iii) police services;

   iv) banks;

   v) medical practitioners;

   vi) credit reference agencies.

d) **Biometrics**. This can give strong verification of real-world identity, but only if there is sound data available to check against. Unlikely to be available to RAs and registrants at present.

e) **Existing relationship**. If an RA already knows an individual, this knowledge may be used instead of, or with other evidence for verifying real-world identity. For example a bank may act as an RA and register existing customers based on its records.

D.2.5 Requirements for specific registration levels

87 The following combinations of evidence are examples that satisfy the registration levels set out in section 3. They are for guidance only and are not to be regarded as an exhaustive list, as other permutations will also be acceptable. They presume that the RA does not already know the registrant.

88 The requirements are different for face-to-face and remote registration, the latter bearing more stringent requirements.

Level 1

Face-to-face registration

89 This requires:

a) a personal statement including:

i) full name of the applicant

ii) date of birth

iii) current permanent address; and

b) at least **one** piece of reputable documentary evidence or third party corroboration.

Remote registration

90 As with face-to-face, but two pieces of documentary evidence/third party corroboration required.

Level 2

Face-to-face registration

91 This requires:

a) a personal statement as for level 1, plus information which may be cross checked against the documentary / third party evidence; and

b) a piece of documentary evidence which contains the registrants signature and photograph (*eg* passport); and

c) one piece of 'active in the community' evidence (two if the real-world identity evidence does not contain a photo and signature).

92 An item of third party corroboration may be substituted for one of the pieces of evidence.

Remote registration (with physical check of documents)

93 This requires:

a) a personal statement as for face-to-face registration; and

b) two items of documentary evidence to verify real-world identity; and

c) two documents demonstrating 'activity in the community'.

94 One or two documents may be replaced by third party corroboration.

Remote registration (with remote corroboration)

95 This requires:

a) a personal statement as for face-to-face, which must cover information to be checked against third party corroboration; and

b) at least two pieces of third party corroboration from separate independent sources.

Level 3

96 At level 3 (real-world identity verified beyond reasonable doubt) remote registration is not encouraged. It may be used only if the RA has the same amount of confidence in the real-world identity, as it would have gained *via* face-to-face registration.

Face-to-face registration

97 This requires:

a) a personal statement, which must include information to be checked against third party corroboration; and

b) at least one piece of documentary evidence to confirm the real-world identity: and

c) two pieces of evidence of activity in the community; and

d) third party corroboration of information in the registrant's personal statement.

Remote registration

98 Remote registration at level 3 will only be permissible if two or more pieces of evidence of both real-world identity and activity in the community are provided, plus third party corroboration from more than one source.

99 Remote registration without physical access to documents is only allowed if strong third party corroboration is obtained from at least four trustworthy sources.

D.3 Registration of organisations and their representatives

100 E-government service providers will follow the guidelines set out by the government for the registration of organisations and their representatives. They are summarised here.

D.3.1 Definitions

101 In this context, real-world identity means a set of attributes that together identify an organisation and/or those attributes that uniquely identify a natural person as representative of an organisation.

102 Validation refers to demonstration that the registrant organisation exists, or that an individual representing an organisation is presenting attributes that actually belong to a real person with some particular role.

103 Verification deals with checking that the registrant organisation or individual is who they claim to be and, in the case of an individual, that they are the true holder of the role.

D.3.2 Scope

104 These guidelines apply to the registration of organisations and their representatives. At the time of registration, it is also necessary to verify that representatives who undertake the registration are who they claim to be and are entitled to register the organisation.

D.3.3 Methods of registration

105 As for registration of individuals, registration is possible by face-to-face or remote interaction.

D.3.4 Types of evidence

106 There are various categories of evidence that may be used in the validation and verification of organisations, some of which are also applicable to the registration of individuals. They are outlined below:

a) **Official registration documents**. This refers to publicly available information registered with an official body (such as annual return and accounts as filed at Companies House). This type of evidence is to be considered the primary means of validating an organisation where possible.

b) **Evidence of dealings with government**. This evidence (such as Pay As You Earn (PAYE) and Value Added Tax (VAT) returns) should be recent and not publicly available. It must also contain evidence of the name and address of the registrant body.

c) **Membership of official or recognised bodies**.

d) **Trading/operational documents**. This evidence is generated in the normal course of business. Examples are invoices, bank statements and internal documents. The documentation must be recent and from a reputable source.

e) **Third party corroboration.** As for the registration of individuals.

f) **General published material**. For example promotional and advertising material, entries in business directories. However, this should only be used in conjunction with other evidence as it is relatively easily spoofed.

g) **Existing relationship**. As for the registration of individuals.

107 The individuals undertaking the registration must verify their real-world identity as described in the guidelines for registration of individuals. Additional evidence must be provided to demonstrate that they are entitled to register on behalf of the organisation. This may take the form of:

a) A signed and dated letter on headed paper from a director or equivalent senior official of the organisation.

b) A digitally signed email from a director or senior official of the organisation, where available.

108 An unsigned email or phone call from a director/senior official may also be used, but it must be noted that these methods do not give a high degree of assurance.

D.3.5 Requirements for specific registration levels

109 The following permutations of evidence, which satisfy particular registration levels, are given for guidance only and are not intended to be exhaustive. They assume that the RA does not already know the registrant organisation.

110 The requirements are given both for face-to-face and remote registration. Of these, some relate to the verification of real-world identity of the organisation and its representative and others to the role and authority of the representative within the organisation. Requirements for remote registration are necessarily more stringent.

111 It is particularly important to identify and check the authority of the registrant's representative in cases where materials containing credentials are to be issued to the representative at the time of registration.

Level 1

Face-to-face registration

112 This requires:

a) at least one official document as evidence of the real-world identity of the organisation; and

b) a short personal statement which identifies the individual and his/her role within the organisation; and

c) evidence of the authority of the individual to act on behalf of the organisation.

Remote registration (by post)

113 Required evidence is as for face-to-face registration, plus a phone call by the RA to the registrant organisation at a known and published number.

Remote registration (online or by phone)

114 In this case, the real-world identity of the registrant organisation is to be verified by an online or telephone enquiry to a trusted provider of company information. The real-world identity and authority of the registrant's representative should be corroborated by contact with the company at a registered or published address and followed by a signed and dated letter of confirmation from a director or senior official.

Level 2

Face-to-face registration

115 This requires:

a) at least two pieces of evidence of the existence of the organisation, including full formal name and address; and

b) evidence of real-world identity of the person authorising the registration as an individual; and

c) a personal statement and corroborating document from the representative identifying him/her and his/her role in the organisation; and

d) a signed and dated document from a director/senior official of the organisation, authorising the representative to undertake the registration. The official should be identified within the documents supplied that support the real-world identity of the organisation.

Remote registration (by post)

116 Required evidence is the same as for face-to-face registration, plus a phone call to the organisation at a known, published number for confirmation.

Remote registration (online or by phone)

117 The RA may confirm the real-world identity of the organisation by reference to remote sources such as Companies House or other registration bodies. The RA will also contact a known and published name and number at the registrant organisation to confirm.

118 Documentary evidence should be submitted to back up the remote registration.

Remote registration (without submission of paper documents)

119 This will only be permissible in cases where it is possible to independently verify the real-world identity of the registrant's representative (*via* third party corroboration)

and where detailed official documents, which verify the real-world identity of the organisation, are accessible remotely.

120 For a limited company, the registrant's representative should be publicly listed as being a director of the organisation. The RA will also obtain third party corroboration of the real-world identity of the representative from at least two sources.

121 In addition the RA will obtain confirmation *via* a phone call to a published number.

Level 3

Face-to-face registration

122 This requires:

a) documentary evidence that includes full formal name and address of the organisation (which should, where applicable, include official registration information); and

b) a piece of evidence to demonstrate that the organisation is still in existence and active; and

c) a personal statement from the representative, giving details of personal real-world identity and relationship with the organisation; and

d) two pieces of evidence which identify the representative as an individual; and

e) a document which identifies the representative in his/her role within the organisation; and

f) a document that authorises the representative to undertake the registration (such as a copy of a board minute certified as true by a company director and secretary). Evidence of the real-world identity of the supplier of authorisation to the representative must be included; and

g) the RA should contact a director (or equivalent) at a published phone number to obtain verbal confirmation.

Remote registration (with submission of documents)

123 This is as for level two, plus an additional piece of evidence to identify the organisation. Also required are two pieces of ID for the representative or two pieces of evidence demonstrating his/her association with the organisation.

Remote registration (without submission of paper documents)

124 Remote registration with no physical access to documents will be considered on a case-by-case basis since the RA must be strongly satisfied of the identities of both the registrant organisation and the representative.

125 In addition to the requirements at level 2, an additional request for registration should be obtained from a second director, whose real-world identity must be verified in the same way as the first.