CABINET OFFICE

Office of the *e-Envoy*

Leading the drive to get the UK online

delivering UK online

HMG's Minimum Requirements for the Verification of the Identity of Individuals

e-Government Strategy Framework Policy and Guidelines

Version 2.0
January 2003

Executive Summary

This note describes HMG's minimum requirements for the validation and verification of an individual's identity as part of the process of issuing a digital certificate or a PIN or Password for use with e-government services.

Record of Changes

Version number	Changes made	Author
0.1	This issue of the document represents a minor update to the *tScheme* guideline[1] for the Verification of the Identity of Individuals in respect of access to Government services. The main change is bringing the document back under HMG control. This issue of the document is for internal government comment.	Office of the e-Envoy
1.0	Updated to reflect comments of C2G and B2G digital certificates stakeholder working groups	Office of the e-Envoy
1.1	Changed format to be consistent with other IAG framework documents	Office of the e-Envoy
2.0	Changes following comments received during public consultation	Office of the e-Envoy

[1] M Leverington, '*Guidelines for the Verification of Identity of Individuals*', TS055_1.0, Pilot Version 01-11-00

Contents

1. Introduction

1.1 Ownership and maintenance

The HMG's minimum requirements for the verification of identity of individuals is one of a series of documents developed as part of the Government's commitment, in the Modernising Government White Paper, to develop a corporate IT strategy for Government. It has been prepared by the Office of the e-Envoy, part of the Cabinet Office, on behalf of the e-Champions.

This document builds on the e-government security policy and the e-government authentication framework policy[2]. It specifically addresses the Government's minimum requirements for the verification and validation of the identity of an individual.

An individual may seek to register for a government service:

a) on their own account; or

b) as a representative of an organisation (natural, corporate or legal).

This document covers the cases where individuals are registering on their own account.

If an individual is registering as a representative of an organisation it is necessary to verify and validate the:

a) identity of the individual;

b) identity of the organisation;

c) authority of the individual to undertake the registration on behalf of the organisation.

This document covers stage a) above, when an individual is registering as a representative of an organisation. The requirements for stages b) and c) are covered in a separate document[3].

This note covers the types of evidence that may be adduced to demonstrate identity attributes and provides guidance on the appropriate mix of evidence for different degrees of rigour.

1.2 Who should read this document?

The document is for Registration Authorities (RA) where the RA is registering individuals partly or wholly in order to facilitate transactions between those individuals and government bodies. It should also be of interest to the providers of citizen to government and business to government transactional services.

---

2 *'e-Government strategy framework policy and guidelines, registration and authentication'*. Available at http://www.e-envoy.gov.uk

3 *'HMG's minimum requirements for the verification of the identity of organisations'*. Available at http://www.e-envoy.gov.uk

It sets out approaches and methods for authenticating individual users at the time at which they are enrolled, in order for them to be issued with credentials, including digital certificates and user name/passwords.

The information within this document may also be of interest to providers of consumer to business and business-to-business transactional services.

1.3 Relationship to *tScheme*

This note describes HMG's registration requirements. A Trust Service Provider (TSP) who wishes to issue certificates that will be accepted by government will need to demonstrate that these requirements are met. *tScheme* provides an approvals scheme for TSPs. As part of the audit of a TSP's service, the *tScheme* auditor will confirm that the requirements specified in this document are being addressed.

1.4 Rationale for this guidance document

Initial registration by the registrant with an RA is a key step to enable the use of electronic trust services by customers and, from the point of view of the registrant, it is potentially one of the most time-consuming and onerous procedures. To encourage public confidence in the process and to facilitate the widest take-up of electronic access to services, it is important that registrants do not have to go through the full registration process every time they need a credential to access a different Government service. The issuance of multiple credentials (e.g. certificates) and/or the use of the same credential by multiple relying parties, will be greatly facilitated if Registration Authorities (and Government bodies) adopt, in so far as is practicable, a consistent approach to the requirements for registration. This is of particular importance where transactions between Government and the citizen are concerned.

1.5 Terminology

Following the Registration and Authentication Framework[2], this note uses the terms validate and verify as follows:

a) **Validate** – demonstrate that a claimed identity exists (i.e. that a person, who has certain attributes, exists);

b) **Verify** – demonstrate that the registrant is whom they claim to be (i.e. that the person purporting to hold these attributes is not impersonating the actual owner of the identity).

In practice, evidence often helps fulfil both requirements simultaneously.

In this note, "identity" means a set of attributes which together uniquely identify an individual.

1.6 Structure of the document

This document is structured as follows:

a) Section 2 discusses the government's requirements for registration.

b) Section 3 describes the acceptable forms of evidence that can be used in verifying and validating an individual's identity.

c) Section 4 describes the evidence that must be presented in order to meet the different Government registration levels.

d) Section 5 highlights a number of potential problems with the registration process and suggests ways in which these problems can be overcome.

2. Requirements Overview

2.1 Introduction

Access to many Government services requires the service user to properly identify him/herself before being granted access. The Government's Registration and Authentication Framework[2] recognises three Registration Levels, depending on the degree of trust required in the asserted identity (for completeness, there is also a level zero where no authentication is required). In allocating transactions to registration levels, the relying party must consider direct and indirect consequences of an asserted identity being called into question.

Full details are in the framework, but in summary:

a) Level One – on the **balance of probabilities**, the registrant's real world identity is verified. An example of a transaction that might merit level 1 registration is the on-line ordering of a publication using a credit card, delivery of which is being made to the credit card account holder's address. In this case failure of the registration process is likely to cause only inconvenience to the real world identity.

b) Level Two – there is **substantial assurance** that the registrant's real world identity is verified. An example of a transaction that might merit level 2 registration is the submission of a VAT return. There must be substantial assurance of real-world identity since the return is legally binding.

c) Level Three – the registrant's real world identity is verified **beyond reasonable doubt**. An example of a transaction that might require level 3 registration is the on-line application for a passport.

The higher the "Registration Level" the greater the assurance that is required in the validation and verification of the registrant. Credentials obtained for Level Two transactions may also be used for Level One transactions, and those obtained for Level Three transactions may also be used for Level One and Level Two transactions.

2.2 Attributes to be validated and verified

Identity means a set of attributes that together uniquely identify a person. Within the UK there is no single "official" or statutory attribute or attributes that is used to uniquely identify individuals across the range of Government bodies. Nor is there an "official" or statutory document or other credential to demonstrate that identity.

However, in almost all cases, an individual will have a set of attributes, which uniquely identify that person across time to a wide range of parties, including Government.

The single attribute that is most often used in a range of contexts to identify an individual is the name(s) by which that person is known.

However other attributes are required to establish a unique identity with any certainty. This is best achieved using other attributes that are recorded and verifiable, not dependent on a specific role, and recognised by a wide range of third parties. These are:

a) Address;

b) Date of birth;

c) If applicable, other names by which a person has been known.

It is through a combination of these attributes by which any given individual is likely to be identified to a wide range of third parties, including Government (sometimes in conjunction with additional specific identifiers).

The minimum set of attributes acceptable to government for specifying the identity of an individual is therefore:

a) Full name or names by which a person is or has been known (including all other names used);

b) Residential Address at which he/she can be located;

c) Date of birth.

Verification involves collecting supporting evidence to verify that these attributes genuinely belong to the registrant. RAs must verify these attributes with a degree of assurance appropriate to the Registration Level claimed in the service description. Other attributes may also be verified if doing so helps to verify the claimed identity. Where an applicant has recently moved house, the previous address should also be validated.

Because no single form of identification can be fully guaranteed as genuine, or representing correct identity, the verification and validation process will in principle be based on the review of various types of evidence, which in combination can confirm the identity of the registrant with a greater or lesser degree of certainty, in a **"cumulative process of identification"**.

There may be other attributes that are relevant to the use of credentials. If such attributes are used, to be useful, these must be associated with a combination of the other attributes outlined above, and evidence adduced to demonstrate that association.

In order to register for a particular government to business or government to citizen transaction service it may be necessary to provide additional attributes (e.g. National Insurance Number, Nationality). These attributes will be ones that, given the level of verification that has already been performed in establishing the identity as part of the process of obtaining a digital certificate, a remote[4] verification process can be used to verify that they genuinely belong to the registrant.

2.3 Records of identification evidence

Records of the supporting evidence and methods used to verify and validate the identity must be retained for a period of 7 years after the end of the business relationship between the individual and the RA. Sufficient records should be kept so that it is possible to reproduce the actual information that would have been obtained during the registration process. Where practical, file copies of the supporting evidence should be retained. Alternatively, the reference numbers and other relevant details of the identification evidence obtained should be recorded to enable the documents to be obtained again. Where checks are

[4] See section 2.5

made electronically, a record of the actual information obtained, or a record of where it can be obtained should be kept.

2.4 Types of evidence to validate and verify an identity

The following types of evidence contribute to validating and verifying an individual's identity, and should be used by RAs.

Types of Evidence	Description	
Personal Statement	Information supplied by Registrant "in his/her own words" or by completing a questionnaire (or supplied by the Registrant's trusted agent in cases where the Registrant cannot do so in person)	
Documents[5]	Documents issued by a third party and in the Registrant's possession (e.g. Passport, Driving Licence, Utility Bill).	
	Main types (not necessarily mutually exclusive)	Evidence of identity per se (normally with photograph and signature)
		Evidence of being "Active in Community" (recent document; shows registrant's address)
Other third-party corroboration from a "Trustworthy Third Party"[6]	Information (as in a reference) obtained by contact between RA and corroborator, or published information	
Existing Relationship	Where the Registrant is already formally known to RA, and has had an official relationship over a substantial period of time (see Section 3.5).	

Table 2-1: Types of evidence to validate and verify and identity

2.5 Methods of Registration

There are three main methods of registration possible. These are:

a) **Face to face** – where the registrant or an agent or proxy meets the Registration Authority or its agents directly;

b) **Remote registration** (in writing, on-line, or by phone), but with presentation of physical supporting evidence;

c) **Remote registration**, and with purely remote (typically on-line) presentation of supporting evidence.

The type and variety of evidence that is adduced may vary between the methods of registration.

5 The acceptable documents are described in section 3

6 The acceptable Trustworthy Third Parties are described in section 3.4

2.6 Verification Requirements

The tables in Section 4 give suitable permutations of minimum evidence for each Registration Level, but these are not exhaustive statements of the possibilities. Other evidence may be used if it gives the requisite level of assurance (see notes below tables).

Section 3 provides examples of acceptable forms of evidence and permutation of evidence at each Level. These do not cover all possibilities and other variations may be acceptable. The RA's service should contact the e-Envoy's Office for additional guidance.

Where existing credentials are used to obtain higher level credentials, the supporting evidence must be additional to that first presented (eg if passport and utility bill were presented to obtain a Level One credential then other proofs of identity must be used to obtain a Level Two credential).

3. Types of Evidence

3.1 Introduction

This section lists examples of suitable evidence that can be adduced to validate and verify identity.

3.2 Personal Statement

3.2.1 Definition

This comprises statements made by, or on behalf of, the registrant concerning his/her identity and history. Capturing all the relevant information will be most easily achieved via a structured questionnaire (in writing, on-line, by telephone, or face-to-face).

It will normally comprise full name or names, date of birth, and permanent address (or contact / care-of address if there is no permanent address).

Other information may be sought if it can be used to help confirm identity. Examples include marital history, educational history, employment, banking details etc.

3.2.2 Use of personal statement

This can serve at least two functions:

a) To uniquely distinguish the individual from any other (to prevent ambiguities or confusion over identity);

b) To provide material which can be checked /confirmed against other classes of evidence. When seeking biographical information, RAs should align the questions asked with the other evidence that is required, so that one can be used to confirm the other and hence give confidence in the identity.

Care must be taken in devising a questionnaire or asking questions. For example, information about the registrant that is not in the public domain, and which the registrant alone is likely to know, can be sought in order to cross check with other forms of evidence. However, care must be taken to avoid being over-intrusive or asking more questions than are required for the purpose, both to ensure conformance with data protection legislation and to maintain confidence of the registrant. Questions and answers that cannot be corroborated by other means or crosschecked against other evidence are of little value and should be avoided.

Confirmation of name and address should be established by reference to a number of sources. The checks should be undertaken by cross validation that the applicant exists at the stated address either through the sight of actual documentary evidence or by undertaking electronic checks of suitable databases or by a combination of the two.

3.3 Documentary Evidence

3.3.1 Introduction

This is defined in this context as documents in the possession of the registrant, which are of a nature to confirm the identity and / or the biography of the individual.

To be of value, these documents should include information on some or all of the attributes of identity referred to above. They should be documents that can only be readily and properly available to the bona fide rightful possessor. The use of documentary evidence is only as reliable as the difficulty of obtaining documents to support a false or misappropriated identity – the easier it is to obtain false documents, the less credence can be placed in that document. As a corollary, the more documents that are required, the higher the potential "hurdle" that an impostor has to overcome.

For convenience, documents may be thought of as comprising two main types, albeit there will be some overlap, and not all documents fit neatly into one or other category. Where more than one document is sought, it is appropriate to seek at least one from each category.

Evidence of identity per se. This will usually hold the registrant's signature, and will in many cases (and preferably) hold the registrant's photograph as well. The signature and photo can be cross-checked against the registrant at the time of registration. An obvious example is a passport.

Other evidence to confirm the identity, address and the "biography" of the registrant (sometimes called evidence of being "active in the community"). This is information that may well not hold the registrant's signature or photo but which will corroborate other information. As a rule, these will be documents which are from a trustworthy source, are dated, and which include the name and where possible the address of the registrant. An example is a bank statement or utility bill.

Where other specific attributes are registered, documentary (or other) evidence must be adduced to associate this attribute with the registrant. For example, a letter from an ISP to a registrant confirming an email address or Web addresses.

To guard against forged or counterfeit documents only originals or notarised copies should be accepted. To guard against the dangers of postal intercept and fraud, registrants should be encouraged to send personal identity documents by a postal service that offers guaranteed delivery (e.g. Royal Mail's Special Delivery service). Alternatively a copy certified by a lawyer, banker or other regulated professional person could be requested.

3.3.2 Examples

Examples of documentary evidence includes the following:

a) Personal identity:

1. current signed passport ;
2. residence permit issued by Home Office to EU Nationals on sight of own country passport;
3. current UK photocard driving licence;
4. current full UK driving licence (old version) – old style provisional driving licences are not acceptable;
5. current benefit book or card or original notification letter from the Department for Work & Pensions confirming the right to benefit;

6. building industry sub-contractor's certificate issued by the Inland Revenue;

7. recent Inland Revenue tax notification;

8. current firearms certificate;

9. birth certificate;

10. adoption certificate;

11. marriage certificate;

12. divorce or annulment papers;

13. Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms);

14. GV3 form issued to people who want to travel in the UK but do not have a valid travel document;

15. Home Office letter IS KOS EX or KOS EX2;

16. police registration document;

17. HM Forces Identity Card.

b) Active in the community:

1. record of home visit;

2. confirmation from an Electoral Register search that a person of that name lives at that address;

3. recent original utility bill or certificate from a utility company confirming the arrangement to pay for the services at a fixed address on prepayment terms (note that mobile telephone bills should not be accepted as they can be sent to different addresses and bills printed from the internet should not be accepted as their integrity cannot be guaranteed);

4. local authority tax bill (valid for current year);

5. current UK photo card driving licence (if not used for evidence of name);

6. current full UK driving licence (old version) (if not used for evidence of name);

7. bank, building society or credit union statement or passbook containing current address;

8. recent original mortgage statement from a recognised lender;

9. current local council rent card or tenancy agreement;

10. current benefit book or card or original notification letter from the Department for Work & Pensions confirming the rights to benefit;

11. court order.

Checking a local or national telephone directory can be used as additional collaborative evidence, but should not be used as a primary check.

Not all documents are of equal value, the ideal is a document that is issued by a trustworthy and reliable source, is difficult to forge, is dated and current, contains the owner's name, photograph, and signature, and itself requires some evidence of identity before being issued (e.g. a passport).

"Active in the community" documents should be recent (at least one should be within the last six months unless there is a good reason why not) and should contain the address and name of the registrant.

3.4 Third Party Corroboration

3.4.1 General

This shall be information supplied normally by a known and trustworthy organisation or person that can confirm (parts of) the biographical statement presented by the applicant. These should be bodies or persons with whom the registrant has recently had a formal, documented relationship. The third party must be independent of the applicant (i.e. **not** be related to the individual).

The distinguishing feature of the third party corroboration is that it should be obtained by bilateral contact between the Registration Authority and the third party, without direct involvement of the registrant other than to give consent and in many cases to propose the identity of the corroborator.

Where practicable such corroboration should include confirmation by the third party of some dynamic information or de facto "shared secret" which is unlikely to be readily known to anyone other than the registrant and the third party.

Third party corroboration can be obtained on-line (in particular, through a digitally signed email), in writing, or by telephone to a published number, or by face-to-face contact.

Each source may be used separately as an alternative to one or more documentary checks. Care must be taken when using a combination of electronic and documentary checks that different original sources of information are used. For example, a physical check of a mortgage statement and an electronic check of the same mortgage account are based on the same source information.

Electronic checks of suitable electronic identity databases are acceptable if the information they hold is derived from one or more suitable sources. Some examples of suitable electronic sources of identity information are:

a) an electronic search of the Electoral Register;

b) access to account databases held by credit reference agencies;

c) an electronic search of public records such as County Court Judgements or bankruptcies;

d) electronic postal address file;

e) postal redirect file.

3.4.2 Issues with third party corroboration

Third party corroboration may be most conveniently obtained through remote access. However, this implies that there is a trusted method of communication between the RA and the third party. This is most readily achievable where there are substantial flows of information between the RA and the third party through an established existing channel.

Consent will usually be required when seeking to process personal data, especially where the data will be disclosed to someone that the data subject did not themselves provide the information.

Some third party corroborators may be reluctant to provide corroboration in case they thereby acquire financial or other liability to the RA (or other parties) for any erroneous corroboration.

These factors may limit the availability of third party corroboration.

3.4.3 Examples of third party corroboration

Examples of possible suppliers of third party corroboration are noted below (this is not an exhaustive list):

a) Government Departments and Agencies (e.g. Public Records Office);

b) Police Force;

c) Utility companies regulated by one of the Regulators;

d) Banks or other financial organisations regulated by the FSA;

e) Medical practitioners with whom the registrant has a formal relationship (e.g. his/her GP);

f) Practising solicitor or barrister with whom the registrant has a client relationship;

g) Practising magistrate or judge;

h) Company or organisation which has been accredited by a *tScheme* member or is itself a *tScheme* member.

Examples of commercial organisations providing acceptable electronic identity services include:

a) Credit Industry Fraud Avoidance System;

b) Dun and Bradstreet Ltd;

c) Equifax Europe Ltd;

d) Experian Ltd;

e) MCL Ltd.

3.5 Existing relationship

Where an individual is already known to a RA or its agent through an existing business relationship, that knowledge may be used in lieu of, or in conjunction with, other evidence to verify identity. For example, a bank, which undertakes the RA role, may choose to register existing customers based on its existing knowledge of those customers. Existing knowledge *may*

give a high degree of assurance in the validation and verification of identity. To do so, it will require that:

a) There is a formal (documented) business relationship between the parties.

b) The RA has confidence that its pre-existing procedures verified the identity of the registrant with sufficient assurance for RA purposes – the RA must be assured that the identity of the registrant is verified to at least the same standard as using other forms of evidence.

c) The information held confirming identity is sufficient and up to date.

d) If the RA does not have sufficient assurance in the registrant's identity then the RA must ensure it uses additional forms of evidence which have not already been presented by the registrant.

4. Requirements for Registration Levels

4.1 Introduction

This section provides Guidance as to the type and variety of evidence that is considered suitable for each of the three Registration Levels.

In reality, there is no single piece of evidence, or combination of evidence, that can conclusively verify an identity. Other things being equal, the more pieces of evidence that are adduced which confirm a registrant's attributes, and the greater the trustworthiness of the sources of evidence, the greater the potential degree of certainty.

The permutations of evidence that may be adduced are for guidance only and cannot provide an exhaustive description of the range of evidence that may suitable. These requirements may be modified, or alternative evidence of identity substituted, if it is appropriate to do so.

The suggestions below assume that the RA does not already know the registrant. As noted above, where the Registration Authority already knows the registrant in a formal capacity, the Registration Authority may use that knowledge in lieu of, or in conjunction with, other evidence.

In all cases, the RA must use staff with the appropriate level of skill in undertaking registration. In particular, in cases where judgements have to be made about the acceptability of alternative evidence or modified requirements, a member of staff of appropriate authority and experience must make the decision and record the reason.

Normally, verification of identity is facilitated by face-to-face registration. Signatures and photographs can be compared, and perceived discrepancies more readily questioned. Under these circumstances, impersonation may be more difficult. For these reasons, this document recommends a greater level of supporting evidence for remote registration than for face-to-face registration.

It should be borne in mind that postal despatch of documents runs a (small) risk of being lost in transit. Registrants should be encouraged to send documents by a postal service that offers guaranteed delivery (e.g. Royal Mail's Special Delivery service). Alternatively copies certified by a trustworthy source (e.g. solicitor, bank, notary) may be used instead of originals for level one and two.

In all cases, the RA must be alert to potential fraud, and information or circumstances that cast suspicion on a registrant's identity.

4.2 Level One

4.2.1 Introduction

There needs to be sufficient checks to have some confidence that the applicant is as claimed, and to deter casual false or misappropriated identities. However, in order to prevent possible inconvenience to registrants, these should not be unnecessarily onerous.

The minimum requirements are described in Table 4-1, with the different columns showing possible permutations of evidence.

Mode of registration		Face to Face			Remote (online/phone)		
Personal Statement (should not be relied upon as evidence of identity)		✔	✔	✔	✔	✔	✔
Documents	**Identity**	✔			✔	✔	
	Active in Community		✔		✔		✔
Third Party Corroboration				✔		✔	✔

Key: each ✔ represents one separate item or source of evidence which must be provided

Table 4-1: Minimum requirements for validation and verification - Level One

Note that a formal documented existing relationship with the RA may substitute for other evidence. Underlying identification checks must have been previously performed and it is essential to ensure that the information used is up-to-date.

4.2.2 Face-to-Face Registration:

Personal Statement

This should include:

a) The full name of the applicant;

b) Date and place of birth (where possible);

c) Current permanent address.

Requiring this information will help to discourage the casual misappropriation of identities / creation of bogus identities.

Other Evidence

At least one piece of reputable documentary evidence or written corroboration of identity from a trustworthy source.

4.2.3 Remote Registration

Personal Statement

As per Face-to-Face registration.

Other Evidence

Two pieces of reputable documentary evidence and / or third party corroboration.

Processes can be relatively mechanistic – there is no requirement to take a detailed history or undertake substantial cross-checking of evidence between history and documentary evidence (although some cross-checking will be required to ensure that the document or corroboration matches the information supplied by the registrant).

Confirmation of the applicant's identity and the fact that the application was made by the person identified can be obtained by:

a) A direct mailing of registration information to a named individual at an independently verified address which is returned completed or acknowledged without alteration to the name or address (care should however be taken to guard against fraudulent change of address information);

b) An initial payment by cheque drawn on a personal account in the applicant's name at a UK or EU bank or building society;

c) Telephone contact with the applicant prior to completing the registration on an independently verified home or business number utilising a minimum of two pieces of personal identity security information that have previously been provided during the set-up process;

d) Internet sign-on following verification procedures where the customer uses security codes, tokens and/or other passwords which have been set up during the registration process and provided by mail (or secure delivery) to the named individual at an independently verified address.

4.3 Level Two

4.3.1 Introduction

The requirements are described in Table 4-2, with the different columns showing possible permutations of evidence.

Mode of registration		Face to Face		Remote (online/ phone)			
Personal Statement (should not be relied upon as evidence of identity)		✔	✔	✔	✔	✔	✔ +
Documents	**Identity**	✔	✔	✔ ✔	✔ ✔	✔	
	Active in Community	✔		✔ ✔	✔	✔ ✔	
Third Party Corroboration			✔		✔	✔	✔ ✔ ✔

Key: each ✔ represents one separate item or source of evidence which must be provided. More than one tick indicates total number of that type of evidence to be provided.
✔ + indicates a higher level of detail required

Table 4-2: Minimum requirements for validation and verification - Level Two

Note that a formal documented relationship may substitute for other evidence, depending on the existing confidence of the RA in the identity of the Registrant. Underlying identification checks must have been previously performed and it is essential to ensure that information used is up-to-date. The use of an existing relationship does not replace the need for a TSP to ensure that it has in its possession and has verified any identification information.

4.3.2 Face-to-Face

Personal Statement

To include the details contained in the Level One, plus information that enables cross-checking of the documents/ third party corroboration.

Other Evidence

One other piece of documentary evidence from a trustworthy source to establish identity must be sought. Where available, such a document should hold the registrant's signature and photograph. Ideally, this should be a passport (or for nationals of countries which issue such documents, a National Identity Document). The advantage of a passport is that it contains the signature and photograph of the holder, and it requires various evidences of identity to be supplied before it is issued.

In addition to this evidence of identity, the registrant must also supply some additional "active in the community" evidence (as defined in section 3). If the "identity" evidence does not contain a photograph and signature, at least two pieces of additional evidence should be sought.

An item of third party corroboration may be substituted for one of the above pieces of evidence, provided that this meets the requirements for such corroboration set out above.

4.3.3 Remote Registration (with physical despatch of documents to an independently verified address)

Personal Statement

A similar personal statement as for face-to-face registration.

Other Evidence

At least two pieces of evidence to demonstrate evidence of identity, plus two separate documents demonstrating "activity in the community."

One or two pieces of documentary evidence may be replaced by third party corroboration.

4.3.4 Remote Registration (with remote corroboration)

Personal Statement

This is similar to that for face-to-face registration, but it must cover information that can be validated against third party corroboration.

Other Evidence

At least two pieces of third party corroboration should be sought from separate independent sources. These must be organisations registered with, regulated and inspected by a statutory British public body and which can corroborate details about the registrant that are unlikely to be known to other persons.

Exceptionally, corroboration from only one third party may be sought, in cases where the RA is able to check elements of the registrant's statement against its own or published records, and that third party has access to a number of sources of information which will be known only to the registrant and those sources. Also, the third party must be able to corroborate a number of pieces of information concerning the registrant that is unlikely to be available to third parties, and which covers a period of time.

4.4 Level Three

4.4.1 Introduction

At Level Three, where the identity of the individual has to be verified beyond reasonable doubt, the authentication requirements are such that remote registration must be used with considerable care. It must only be allowed if the RA is satisfied that the certainty as to identity is at least as strong as would be obtained using face-to-face registration. The reason for allowing remote registration must be decided on a case-by-case basis by the RA and recorded by the RA. In particular, the Information Commissioner has advised that remote registration should not be used

for individuals where this registration could permit access to personal information that could then be manipulated. This is to protect against fraudulent access to someone else's personal data.

The requirements for Level Three are described in Table 4-3, with the different columns showing possible permutations of evidence.

Mode of registration		**Face to Face**		**Remote (online/phone) To be used with care: see main text**	
				With physical supporting evidence	Without physical supporting evidence
Personal Statement (should not be relied upon as evidence of identity)		✔ +	✔ +	✔ +	✔ +
Documents	**Identity**	✔ ✔	✔	✔ ✔	
	Active in Community	✔	✔	✔ ✔	
Third Party Corroboration		✔	✔ ✔	✔ ✔	✔ ✔ ✔ ✔

Key: each ✔ represents one separate item or source of evidence which must be provided. More than one tick indicates total number of that type of evidence to be provided.
✔ + indicates a higher level of detail required.

Table 4-3: Minimum requirements for validation and verification - Level Three

Note that a formal documented relationship may substitute for other evidence, only if the RA already has strong confidence in the identity of the Registrant. Underlying identification checks must have been previously performed and it is essential to ensure that information used is up-to-date. The use of an existing relationship does not replace the need for a TSP to ensure that it has in its possession and has verified any identification information.

4.4.2 Face to Face

Personal Statement

A personal statement should include sufficient information to be checked against third party corroboration.

Other evidence

At least one piece of documentary evidence to confirm identity, plus two of being active in the community is required. In addition, third party corroboration should be obtained and cross-checked with the registrant's personal statement. If data protection reasons make it impracticable for the RA to seek third party corroboration directly, the registrant may provide a document him/herself from a third party. Such a third party must be professionally known to the registrant, and the existence of such a third party must be verifiable by the RA. Further information should always be sought in the case of any doubt or inconsistency.

4.4.3 Remote Registration

Remote registration must only be undertaken at level three if more than one piece of documentary evidence of both identity and activity in the community can be provided, plus third party corroboration from more than one source. Further information should always be sought in

the case of any doubt or inconsistency. (See the caveats above concerning remote registration at Level Three.)

Remote registration without submission of documentary evidence may only be used if strong corroboration of identity can be obtained from several (at least four) different trustworthy sources already known to the RA, and which can corroborate evidence that realistically can only be known to the registrant and the corroborator. In these situations, advice should be sought from the Information Commissioner.

5. Problems and Issues with Registration

5.1 Wider use of certificates

HMG is keen that certificates issued to support access to government services should also have wider applicability. In producing this document the Identification Evidence required by financial organisations under Money Laundering regulations has been reviewed. The level 2 profile presented in this report meets the identification requirements presented in the Joint Money Laundering Steering Group's guidance. However for high risk financial activities or customers conducting large transactions it maybe appropriate for a financial organisation to require the level 3 requirements to be met.

For certain enrolment processes, such as opening a bank account, it may be necessary in some cases to "look behind"[7] the identity of the Registrant to enable the underlying beneficial owners of funds to be identified. However, this is not the responsibility of the Registration Authority, it will be for the relying party (whether a government department or otherwise) to institute checks if such are thought necessary. This could perhaps be "subcontracted" to the Registration Authority, but this would be an additional contractually separate service over and above the registration process per se. The responsibility of the Registration Authority is to establish the identity but not to look behind it.

5.2 Access to Registration Authorities

As noted above, at Level Three in particular, registration is preferred to be by face-to-face contact. However, this can present difficulties in some cases, for example:

a) in certain cases of disability or medical conditions, and / or where the Registrant is housebound;

b) where the Registrant lives in a physically remote location;

c) where the Registrant regularly works abroad or in some other "inaccessible" location for long periods (e.g. offshore);

d) in other situations where a Registrant is likely to find it difficult to present in person during "normal" hours at a "normal" business location.

This presents challenges for Registration Authorities who aim to ensure inclusivity and wide availability of their services.

---

[7] See for example *'Money Laundering Guidance Notes for The Financial Sector'*, 2001 Edition, Joint Money Laundering Steering Group.

5.3 Potential solutions

It is for each Registration Authority to determine the best way to respond, bearing in mind the need to ensure that the degree of assurance as to the registrant's identity is not compromised. However, potential solutions are suggested here.

a) The Registration Authority's staff travel and undertake visits away from their normal place of business to meet Registrants face-to-face.

b) A third party acts as agent for the Registrant and presents face-to-face at the Registration Authority on behalf of the Registrant. Ideally, this person should be someone who is himself/herself registered to Level 3, is of appropriate professional standing, and is personally known to the Registrant in a professional capacity and not have a potential conflict of interest.

c) The authority for the representative to act on behalf of the Registrant must be clearly documented. For Levels 1 and 2, this should comprise a signed letter from the Registrant (or if applicable, official authority such as Power of Attorney, etc). For Level 3, an additional trustworthy third party should countersign the letter, or additional independent confirmation sought from the registrant by the RA that the letter is genuine.

5.4 Availability of documentation

As well as the problem of personal access to RAs alluded to above, there is also the problem of those individuals who for a variety of reasons may not have access to a wide range of identification documents. For example, someone who does not drive, has not travelled abroad for many years if ever, does not own or rent property in their own name, is not in employment and does not hold a bank account, may find it difficult to provide many of the kinds of documentary evidence suggested as proof of identity.

This difficulty may be particularly acute with some social groups (e.g., the homeless and other "dispossessed" or socially excluded persons). However, a wide segment of the population will lack at least some of the documentation. Furthermore, some groups (e.g. some elderly people) and those with certain types of disability or illness who may find it difficult to present in person, may also be disproportionately likely to lack much documentation.

5.5 Potential solutions

In these cases Registration Authorities may need to use visiting staff and/or agents. A vigilant but pragmatic approach to the acceptability of "non-standard" documentary evidence will be needed, plus full use of third party corroboration. The very absence of documents may add credence to a registrant's story (but of course, one cannot prove that the registrant is not withholding documents). For example, a TSP may accept as identification evidence a letter or statement from a person in a position of responsibility who knows the client, that tends to show that the applicant is who he/she says he/she is and to confirm his/her permanent address if he/she has one. Examples of persons in a position of responsibility include solicitors, doctors, ministers of religions, teachers, hostel managers and social workers.

It may be noted that visiting the registrant at home is of itself a useful technique in giving assurance to the claimed identity (at the least, it strongly indicates that the purported registrant has access to the registrant's home address).

5.6 Additional authentication by relying parties

This guideline is for the guidance of Registration Authorities, in particular, when registering individuals with a view to facilitating access to Government. However, in many cases a relying party (in Government or otherwise) will also be in a position to undertake some additional verification from their own records when a customer presents with a credential. As noted previously, verification of identity is a cumulative process. As such, the relying party may gain additional assurance through undertaking its own independent verification. This may be done using a “shared secret” (i.e. a piece of information that should be known only to the relying party and the registrant).

5.7 Storage and processing of information

As a result of registration and authentication activities, Registration Authorities will come to hold personal data on registrants. Registration Authorities are required to adhere to the requirements of all relevant legislation in their dealing with this data. In particular, the privacy and security of all personal information obtained during the registration process is paramount.

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

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