



Office of the *e-Envoy*

Leading the drive to get the UK online

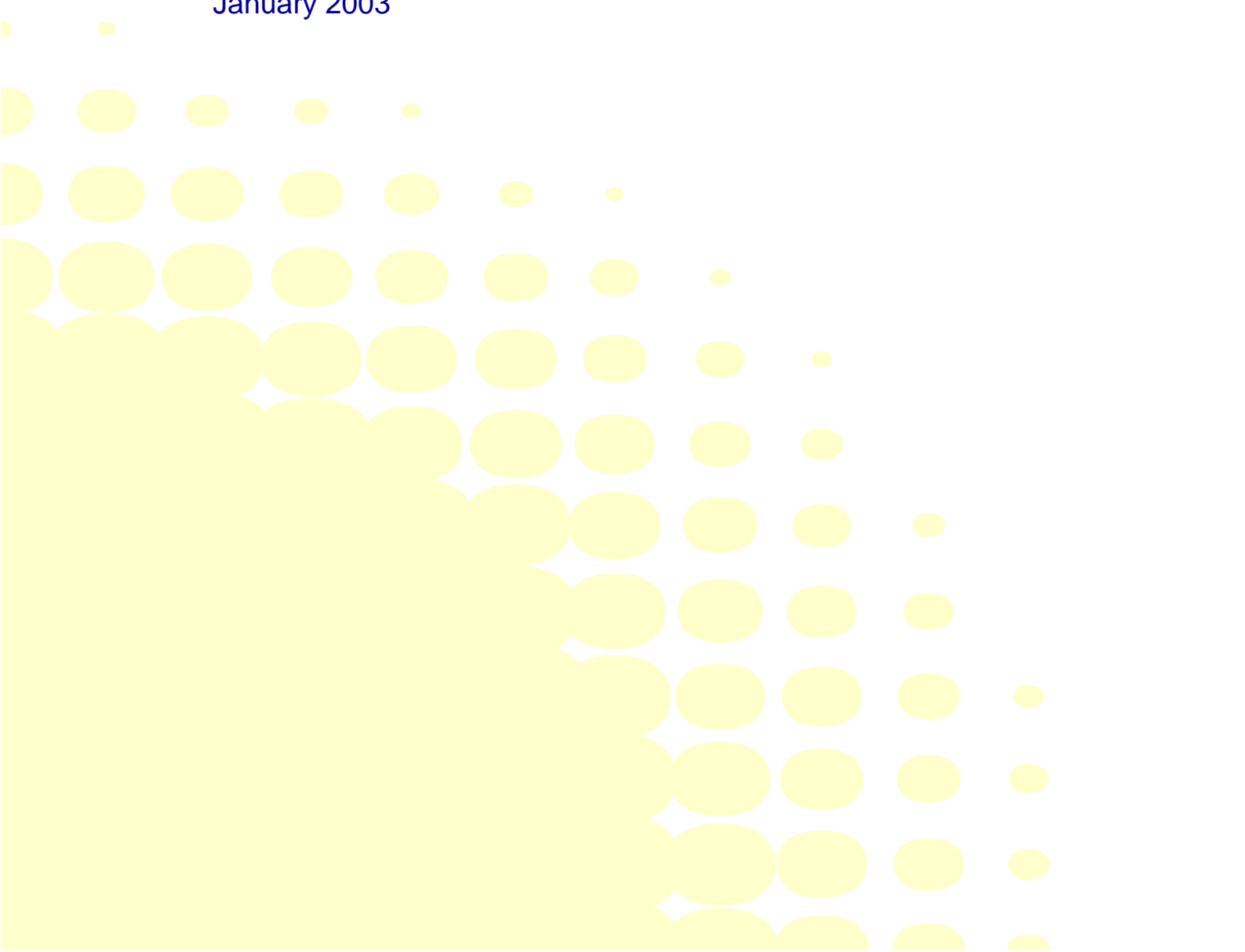
delivering



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

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 organisation'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 <i>tScheme</i> guideline for the Verification of the Identity of Organisations 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 from the C2G and B2G stakeholder working groups	Office of the e-Envoy
1.1	Format changed to bring it in line with the IAG framework documents	Office of the e-Envoy
2.0	Changes following comments received during public consultation	Office of the e-Envoy

Contents

Executive Summary	2
Record of Changes	3
1. Introduction	7
1.1 Ownership and maintenance	7
1.2 Who should read this document?	8
1.3 Rationale for this Guidance Document	8
1.4 Relationship to <i>tScheme</i>	8
1.5 Terminology	8
1.6 Structure of the document	9
2.3 Types of Evidence to validate and verify an Identity	12
2.4 Methods of Registration	14
2.5 Records of identification evidence	14
2.6 Verification requirements	14
3. Types of Evidence	17
3.1 Introduction	17
3.2 Evidence of identity of the organisation	17
3.3 Evidence of Identity for registrant's representatives	21
3.4 Evidence of authority	21
4. Requirements for achieving validation and verification	23
4.1 General	23
4.2 Level One	23
4.3 Level Two	25

4.4	Level Three	27
5.	Problems and Issues with Registration	31
5.1	Wider application of certificates	31
5.2	Controlling interests in registrant organisations	31
5.3	Additional authentication by relying parties	31
5.4	Storage and processing of information	32

1. Introduction

1.1 Ownership and maintenance

The HMG's minimum requirements for the verification of the identity of organisations 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 policy¹. It specifically addresses the Government's minimum requirements for the verification and validation of the identity of an organisation. In this context, an organisation includes:

- a) Registered Companies;
- b) Other corporate bodies;
- c) Partnerships;
- d) Other unincorporated bodies and associations.

The term "organisation"² is employed in a generic sense in this document to refer to all the above-mentioned types of bodies. Where specific requirements or processes apply to specific types of organisation, these are noted as necessary.

When 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 describes HMG's minimum requirements for verifying and validating the identity of the organisation and for verifying and validating that the individual undertaking the registration has the authority to do so. A companion document, HMG's minimum requirements for the verification of the identity of individuals³, describes HMG's minimum requirements for verifying and validating the identity of the individual (stage 'a' above). This latter document should be followed in verifying the identity of the representative(s) of an organisation.

¹ 'e-Government strategy framework policy and guidelines, registration and authentication'.

Available at <http://www.e-envoy.gov.uk>

² Note that a 'sole trader' should be considered as an individual.

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

Note that the minimum requirements specified in this document are applicable to the registration process for the issuance of digital certificates **and** PINS/Passwords that will be used in authenticating users of business to government (B2G) services.

1.2 Who should read this document?

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

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

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

1.3 Rationale for this Guidance Document

Initial registration by the registrant with an RA is a crucial step to enable the use of electronic trust services, 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 trust 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. digital certificates), and/or the use of the same credential by multiple relying parties, will be greatly facilitated if RAs (and Government bodies) adopt a consistent approach to the requirements for registration.

Other organisations may find this document useful in determining whether they are happy to rely on certificates issued to support business to government transactions.

1.4 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.

1.5 Terminology

Following the Registration and Authentication Framework¹, this note uses the terms validate and verify as follows:

- a) **Validate** – demonstrate that a claimed identity exists (i.e. that an organisation exists which has certain attributes);
- b) **Verify** – demonstrate that the registrant organisation is the one claimed (i.e. that the organisation purporting to hold these attributes is not being misrepresented).

In practice, evidence often helps fulfil both requirements simultaneously.

In this note, “identity” means a set of attributes which together uniquely identify an organisation.

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 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 could be overcome.

2. Requirements Overview

2.1 Introduction

Access to many Government services requires the service user to identify himself/herself and the organisation that they represent, before being granted access. The Government's Registration and Authentication Framework¹ recognises three Registration Levels, depending on the degree of trust required in the asserted identity⁴. In deciding on the Registration Level appropriate for a transaction, 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 identity is verified. An example of a transaction that might merit level 1 registration is the on-line ordering of a publication using a Company credit card, delivery of which is being made to the company'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 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 a request to gain access to information from the Criminal Records Bureau.

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 an organisation (natural, corporate or legal). Within the UK there is no single "official" or statutory attribute or set of attributes that is used to uniquely identify organisations across the range of Government bodies. Nor is there an "official" or statutory document or other credential to demonstrate that identity. Most organisations (and individuals) will have a set of attributes, some or all of which uniquely identify them to a wide range of parties, including government.

It is not possible to give a definitive list of all the attributes that may be used to define an identity in all cases, but guidance is noted below. As a minimum, this will include the name by which an organisation is known and the address at which it undertakes its activities.

⁴ There is also a level zero where no authentication is required.

Corporate organisations have certain legally required attributes, which can be regarded as defining identity. The identity of a corporate organisation includes its:

- a) registered number;
- b) registered corporate name and any trading names used;
- c) registered address and any separate principal trading addresses.

These are recorded in statutory declarations at Companies House.

Certain other organisations also register with official statutory or other governing bodies. In this case, it will be the attributes by which they are known and recognised to such bodies that will be required.

One particular attribute, which often acts as a de facto “official” registration for most trading bodies, is the VAT registration number. This should be verified where appropriate.

Government relying parties (and many other relying parties) will need these “core” attributes to be verified if they are to have confidence in a credential. Other additional meaningful attributes may be needed in certain cases, depending on the use to which the certificate will be put.

As well as verifying the registrant organisation itself, it is necessary to verify the identity of the registrant’s representatives who undertake the registration. This is to ensure that they are who they claim to be, and are actually entitled to register their organisation. This is particularly important where a credential (e.g. media containing a digital certificate or key pair) is issued directly to the representative at the time of registration.

In summary, authentication at registration shall contain the following elements:

- a) Validating and verifying the identity of the registrant organisation;
- b) Verifying the identity of the registrant’s representative undertaking the registration;
- c) Demonstrating that the representative is affiliated to the organisation;
- d) Verifying that they have the authority to undertake the registration on behalf of the organisation.

This helps to ensure that credentials are not issued to impostors purporting to have a role in an organisation, and also to ensure that registration is denied to persons who do belong to an organisation, but who have no authority to commit that organisation.

2.3 Types of Evidence to validate and verify an Identity

Achieving validation and verification will require that the registrant provides evidence of identity that an impostor would have difficulty in obtaining or acquiring. Other things being equal, the more evidence that is required, the more difficult it is to misappropriate an identity, therefore the greater the assurance in that identity. Because no single form of identification can be fully guaranteed as genuine, or representing the correct identity, the verification process must be cumulative.

Table 2-1 lists the types of evidence that can be used to validate the identity of an organisation. Table 2-2 lists the types of evidence that can be used to validate the identity of registrant’s representatives (RR) and their authority to represent the organisation. This person has to have

their personal identity confirmed to the level required as described in the registration framework for individuals³.

	Generic Types of Evidence	Description	Comment
1	Public Registration/ Licences/Official Filings	The organisation has registered with an official registration body, and submits publicly available documents (e.g. a Ltd company at Companies House, a Registered Charity with Charity Commissioners etc). Public licences to operate, where applicable	The most authoritative method of establishing identity. To be used wherever possible (but not applicable in some cases e.g. partnerships)
2	Dealings with Government	Information supplied to government departments or other official bodies which are not publicly available (e.g. tax, VAT, PAYE returns etc)	Helps to confirm ID in lieu of (1)
3	Membership	Evidence of membership of a known trade association, affiliation to recognised professional body, or other body	Helps to confirm ID in lieu of (1) if the identity has been verified by the trade association.
4	Trade/operational documents	Material generated by the organisation in the course of its activities, but which are not public knowledge (invoices, internal documents etc).	Helps to establish Registrant's representative as a bona fide representative and to confirm details of premises, etc
5	Third Party Corroboration from a "Trustworthy Third Party"	Information obtained by bilateral contact between RA and third party	
6	Publications	Material produced for public consumption in course of activities.	Helps to confirm ID in lieu of (1), and to confirm premises etc in addition to (1)
7	Existing Relationship	Where the Registrant Organisation is already known to RA in a formal capacity	If the identity of the Registrant has already been properly verified by the RA, this can give a high degree of assurance as to ID

Table 2-1: Examples of the evidence that can be used to validate the identity of an organisation

Documentary evidence provides one source that can be used to validate and verify an identity. Documentary evidence is however, not the only method of achieving verification. Direct corroboration from a trustworthy third party may also be used; and where the RA already knows the registrant organisation and its representatives, this may be used in lieu of (some of) the other evidence. In such cases, the nature of the existing relationship between the RA and the registrant must be formally documented and the reason for accepting this as evidence must be recorded.

	Generic Types of Evidence	Description	Comment
1	Documentary evidence of ID	Current (up to date) evidence of the RR's identity normally with photo and signature	E.g. passport, official ID card
2	Documentary evidence of affiliation	Demonstrates that the RR is associated with the organisation	To be of use, needs to be current. (e.g. Letter of appointment, wage slip, P60 etc)
3	Documentary Evidence of Authority	Demonstration that the RR is empowered to act on behalf of the Registrant organisation	Must be dated and issued by an appropriate, named person. (At Level Three, a board resolution or equivalent)
4	"Back Contact" with Registrant organisation	Contact between RA and the registrant organisation, independent of the RR	To be of weight must be to trustworthy contact point and known contact

Table 2-2: Evidence that can be used to verify the identity of a registrant's representative

2.4 Methods of Registration

There are three main methods of registration. These are:

- a) **Face to face**, where the registrant organisation's representatives (or an agent) meets the Registration Authority (or its agent) directly.
- b) **Remote registration** (in writing, on-line, or by phone), but with presentation of physical supporting evidence to the RA.
- c) **Remote registration** with purely remote (especially on-line) presentation of supporting evidence.

The type of evidence that is adduced will vary between the methods of registration.

2.5 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 organisation 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 re-obtained. Where checks are made electronically, a record of the actual information obtained, or a record of where it can be re-obtained should be kept.

2.6 Verification requirements

Because no single form of identification can be fully guaranteed as genuine, or representing correct identity, the identification process will need to be cumulative.

Section 4 gives suitable permutations of minimum evidence for each Registration Level, but is not an exhaustive statement of the possibilities. These permutations assume the evidence meets the requirements set out in Section 3 below.

3. Types of Evidence

3.1 Introduction

This section lists examples of suitable evidence that can be adduced to validate and verify identity. It is organised into a discussion of the requirements for:

- a) evidence of the identity of the organisation;
- b) evidence of identity for registrant's representative;
- c) evidence of authority.

3.2 Evidence of identity of the organisation

3.2.1 General

In order to validate and verify identity, it is necessary for suitable evidence to be supplied by the registrant organisation.

Table 2-1 lists some of the types of evidence described below that may be adduced to validate and verify the identity of an organisation. For convenience, these are grouped into categories. Some of these are likely to give a higher degree of assurance than are others and this is noted where appropriate.

The types of evidence listed below are particularly relevant where the registrant organisation is based in the UK. However, similar or analogous documents will usually be available for foreign organisations that wish to register.

3.2.2 Official Registration Documents

These are publicly available information filed or registered with an official body. Examples include:

- a) Partnership deed;
- b) The original⁵ or certified copy of the Certificate of Incorporation;
- c) Certified copy of the Form 12 Statutory declaration of incorporation.

For "level two" and above, the Company Secretary or a solicitor or notary should certify copies.

In general, validating the existence of a limited company beyond reasonable doubt is quite straightforward, particularly if it has been in existence for some time. This type of information is the most authoritative (and relatively straightforward) method of establishing the existence of a

⁵ To guard against the dangers of postal intercept and fraud, registrants should be asked to send original documents using a postal service that provides guaranteed delivery (e.g. Royal Mail's Special Delivery).

body. In most cases it can be undertaken remotely (e.g. by online search of Companies House records).

Other organisations may similarly be registered with official or statutory governing bodies. Registered charities will be registered with the Charity Commissioners, firms of solicitors with the Law Society, etc.

Official registration as described above should be the primary means of validating an organisation where possible.

3.2.3 Evidence of Dealings with Government

This comprises information supplied to government departments or other official bodies in the course of business, but which is not publicly available. Examples include:

- a) Tax returns;
- b) PAYE records;
- c) VAT registrations/ returns;
- d) Unified Business Rate account.

To be of value, such evidence needs to be recent (preferably the most recent example), must contain evidence of the name and address of the registrant body, and be the original or a copy certified by an identified director of the organisation.

If a representative of a body can present such documents, it is evidence both of the existence of the organisation itself, and gives some assurance that the representative is likely to be genuine.

3.2.4 Membership of official or recognised bodies

Examples of relevant evidence include:

- a) evidence of membership of trade organisations, affiliation to professional bodies or other bodies. Where organisations are branches or members of a wider organisation (e.g. a religious body) this may include the HQ of that wider organisation.
- b) evidence of membership of CBI, Chambers of Commerce, industry-specific organisations, etc.

This material helps to confirm the existence and identity of an organisation, and may also be able to provide details of the officers of the organisation.

3.2.5 Trading/operational Documents

Trading/operational documents are material generated in the course of an organisation's activities. Most companies and organisations will have substantial documentation from their course of business that can be adduced to confirm their identity. Examples include:

- a) Invoices, bills, receipts etc to customers and from suppliers;
- b) A wide range of internal business documents;
- c) Bank Statements.

To be of value this material needs to be recent (<6 months old), original, and itself from a source the identity of which is not in question.

3.2.6 Third Party Corroboration

This is information/confirmation directly supplied to the Registration Authority by a third party, to back up the registrant's claim. Possible sources include:

- a) Government Departments and Agencies (including Companies House);
- b) Local Authorities;
- c) Banks or other organisations regulated by the FSA;
- d) Credit reference agencies;
- e) Established "trustworthy" company or other body (such as a utility) with whom the registrant body has a professional relationship.

Confirmation of the validity of a VAT registration number may be obtained from <http://europa.eu.int/comm/taxation-customes/vies/en/vieshome.htm>. The HMC&E National Advice Service may also be able to confirm the validity of a VAT registration number.

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.

Depending on source, this may provide a useful substitute or additive evidence, especially for small, unincorporated organisations. The value / evidential weight of such corroboration will depend on the source. It may be available remotely.

In practice, cost, liability, and data protection issues may limit availability of corroboration from some sources. For data protection reasons, third parties may be unable to release information to a RA unless the third party has explicit consent from the data subject (registrant). In addition to any data protection issues, some third parties may be reluctant to provide corroboration in case they thereby acquire financial or other liability to the RA or other parties in respect of any false corroboration.

One type of third party corroboration that may be available in respect of some identities is provided by certain credit reference agencies, which may also provide a service for verifying identity based on information held by the agency. This information may be derived from information supplied with the registrant's organisations financial history (financial information per se should not be disclosed to an RA) and other material.

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 Register of Companies produced by Companies House;
- b) Access to account databases held by credit reference agencies;

- c) An electronic search of public records such as County Court Judgments or bankruptcies;
- d) Electronic postal address file;
- e) Postal redirect file.

3.2.7 General published material

This may be defined as material produced for public consumption in the course of business/activity. Examples include:

- a) Promotional and advertising material with names, address, and phone numbers;
- b) Entries in business directories, Yellow Pages, etc.

This information helps to confirm identity in lieu of other information and to confirm the organisation's place of business. This information may be available remotely (e.g. a website). However, it should not be used without additional evidence as proof of validation or verification as it is relatively easy to spoof, and may not give full details of the identity of the company or organisation.

3.2.8 Existing relationship

Where an RA or its agent already knows an organisation and its representatives 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 that undertakes an RA role may choose to register existing customers based on its existing knowledge of those customers. In some circumstances existing knowledge may give a high degree of assurance in the validation and verification of identity. This will require that:

- a) There is a formal (documented) business relationship between the parties.
- b) The RA must have 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.

The use of an existing relationship does not replace the need for the TSP to ensure that it has in its possession, and has verified, identification information.

3.2.9 Issues concerning the identity of a registrant body

It should be noted that confusion can sometimes arise between organisations, (e.g. limited companies) especially where there is a Group with a parent company and one or more subsidiaries, some of whom may have the same registered office and/or trading addresses, and very similar names. In these circumstances, it is essential to ensure that one is in fact registering the correct company. In particular, for a limited company, the registered number should always be verified and recorded as part of the registration process.

Some corporate bodies may use other trading names, and different or additional addresses, from those recorded in official registration documents. When RAs record such alternative names and addresses for registration purposes, evidence must be presented which verifies these alternative names and addresses.

3.3 Evidence of Identity for registrant's representatives

As noted previously it will be necessary for the individuals who are undertaking the registration activity on behalf of an organisation to verify their identity. HMG's minimum requirements for verifying an individual's identity, described in reference 3, should be met in verifying their identity.

3.4 Evidence of authority

As noted before it is also essential to verify that the individuals who are undertaking the registration activity on behalf of an organisation have the authority to do so. This evidence may be provided by:

- a) A signed and dated letter on headed paper from a director or equivalent senior official of the organisation.
- b) A digitally signed email, (supported by an existing digital certificate), from a director/senior official of the organisation. An email from a director/senior may be used, but care must be taken, as unless it is digitally signed, an email does not have a high degree of assurance as to its authenticity and integrity.
- c) A telephone call to a known number to seek confirmation from a director/senior official may be used, but care must be taken with this method. The confidence that can be placed in such verification may be less than with a written document, and unless recorded, a telephone call does not give an auditable record.

4. Requirements for achieving validation and verification

4.1 General

Guidance as to the type and variety of evidence that may be suitable is noted below. 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, 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 necessarily cannot provide an exhaustive description of the evidence which may be 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 before, 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.

Verification of identity is facilitated by face-to-face registration. Signatures and photographs can be compared, and perceived discrepancies more readily questioned. 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 postal service that offers guaranteed delivery (e.g. Royal Mail's special delivery service). For levels One and Two, copies of documents certified by a trustworthy source (e.g. solicitor, bank, notary) may be used instead of originals.

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

4.2 Level One

4.2.1 Introduction

At level one verification of an organisation and its representatives is adequate if based on the balance of probabilities of being correct.

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

The minimum requirements are described in Tables 4-1 (for registrant organisations) and 4-2 (for registrant's representative), with the different columns showing possible permutations of evidence.

Mode of Registration	Face to Face			Remote (online/telephone)		
Public Registration (<i>to be used as the primary source where possible</i>)	✓			✓		
Dealings with Government/ Membership /Trade/Operational		✓			✓ ✓	✓
Third Party Corroboration			✓			✓

Key ✓ = Must be provided. More than one tick indicates total number of that type of evidence to be provided.

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

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

Mode of Registration	Face to Face			Remote (online/telephone)		
Evidence of ID	(1)	(1)	(1)	✓		✓
Evidence of affiliation with the organisation	(1)	(1)	(1)		✓	✓
Evidence of authority to act for the organisation	✓	✓	✓	✓	✓	✓
"Back Contact" with Registrant Organisation				✓	✓	

Key ✓ = Must be provided
(1) = One of the items from the list must be provided

Table 4-2: Minimum requirements for validation and verification of registrant's representative - Level One

4.2.2 Face to face

Registrant organisation

At least one piece of evidence of the identity of the organisation from an official document.

Registrant's representative

A brief personal statement identifying the individual and his/her role in the registrant organisation. Other evidence required is described in reference 3.

Authority

Evidence of the authority conferred on that individual to act on behalf of the company is required. This could be a letter on headed paper signed by a director.

4.2.3 Remote Registration (by post)

The same evidence as per face-to-face registration is appropriate, plus a telephone call by the Registration Authority to the registrant organisation at a known and published number.

4.2.4 Remote Registration (online or by telephone)

Registrant organisation

Where registration is undertaken remotely (typically by telephone or on-line), an on-line or telephone enquiry to Companies House or an established provider of on-line company information may be contacted to validate the identity of the Registrant Company.

Registrant's representative and authority

In order to corroborate the identity of the registrant's representative, contact should be made with the registrant company at its registered office or other published address, to confirm the bona fides of the representative (using some "shared secret" between the registrant company and the registrant's representative). This contact may be via telephone or email. A signed and dated letter should follow it from a director/senior official of the company confirming the intention to register.

4.3 Level Two

4.3.1 Introduction

At level two it is necessary to validate and verify the identity of the company or organisation and its representative with a substantial degree of assurance.

The minimum requirements are described in Tables 4-3 (for registrant organisations) and 4-4 (for registrant's representative), with the different columns showing possible permutations of evidence.

Mode of Registration	Face to Face			Remote (online/telephone)	
Public Registration (<i>to be used as the primary source where possible</i>)	✓			✓	
Dealings with Government/ Membership /Trade/Operational		✓ ✓	✓		✓ ✓
Third Party Corroboration			✓		✓

Key ✓ = Must be provided. More than one tick indicates total number of that type of evidence to be provided.

Table 4-3: Minimum requirements for validation and verification of registrant organisation - Level Two

Note that a formal documented existing relationship with the RA may be used in lieu of / with other evidence only if the RA already has strong confidence in the identity of the registrant organisation. 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.

Mode of registration	Face to Face		Remote (online/telephone)
Evidence of ID	✓	✓	✓
Evidence of affiliation with the organisation	✓		✓
Evidence of authority to act for the organisation	✓	✓	✓
“Back Contact” with Registrant Organisation		✓	✓

Key ✓ = Must be provided

Table 4-4: Minimum requirements for validation and verification of registrant's representative - Level Two

4.3.2 Face to face

Registrant organisation

Evidence of the existence of the organisation, to include full formal name and full address (at least two pieces of evidence unless formal “official” filings are used), and the identity of the person authorising the registration.

Registrant's representative

A personal statement identifying him/her and his/her role in the organisation. Other evidence required is described in reference 3.

Authority

At minimum, the registrant's representative is required to supply a document that identifies him/her in his/her capacity as a director/employee of the company, and an additional document verifying the identity of the representative as an individual.

It is of particular importance to positively identify the registrant's representative in cases where media or material containing or storing any credentials are to be issued to the registrant's representatives at the time of registration.

Also needed is a signed and dated document on Company headed paper from a director/manager of the company, authorising the named representative to undertake the enrolment. The individual who provides the authorisation should be identified as such within the documents supplied supporting the identity of the company (e.g., his/her name should be in the list of directors).

4.3.3 Remote Registration (by post)

The evidential requirements are similar to face-to-face registration, plus the Registration Authority should telephone the organisation at a known, published number to seek confirmation.

In this case the evidential requirements will include a signed resolution of the directors or equivalent, authorising the registration, accompanied by additional documentation confirming the identity of the company. The identity of the individual who is undertaking the registration activity should be clearly stated, and evidence associating him/her with the company should also be adduced. In verifying the identity of the individual undertaking the registration process the requirements specified in reference 3 should be met.

4.3.4 Remote Registration (online or by telephone)

Following the initial request for registration, the Registration Authority may confirm the identity of the organisation by access to remote sources such as Companies House or other appropriate

Registration bodies. The Registration Authority shall make telephone contact to a known and published name and number at the registrant organisation.

Documentary evidence should be submitted to back up the remote registration. This should include certified copies of the certificate of incorporation or other similar evidence and a written record of the decision to enrol.

4.3.5 Remote Registration (without submission of paper documents)

This should only be undertaken where it is possible to independently verify the identity of the registrant's representative making the request. This will require the availability of third party corroboration. Also, remote registration without submission of paper documents can only be undertaken where there are detailed official documents, accessible remotely, which can unambiguously validate the organisation's identity. For example, registration at Companies House.

The RA must be satisfied as to the identity of the person undertaking the registration. The requirements specified in reference 3 should be satisfied.

The authority of the individual to perform the registration needs to be validated. For a limited company this will require that the registrant's representative should be publicly listed as being a director of the Registrant Company or organisation. The RA will need to obtain independent third party corroboration as to the identity of the registrant's representative, from at least two sources. This will require checking information that will realistically be known only to the representative and to the bodies that supply the corroborative evidence. It should be noted that significant information about the directors of a registered company is in the public domain and accessible through Companies House. Any third party corroboration must necessarily cover material that is not publicly available.

It will be appropriate for the RA to seek additional telephone confirmation from a published number, bearing in mind the caveats concerning the value of telephone confirmation.

4.4 Level Three

4.4.1 Introduction

At Level Three, the Authentication requirements are onerous as it is necessary to verify and validate the identity beyond reasonable doubt. Remote registration may be undertaken only if the RA is fully satisfied that the certainty as to the registrant's identity is sufficiently strong. The reason for allowing remote registration must be decided on a case-by-case basis by the RA and recorded by the RA. It will be most easily facilitated in those cases where the RA already knows the registrant organisation and its representatives.

The minimum requirements are described in Tables 4-5 (for registrant organisations) and 4-6 (for registrant's representative), with the different columns showing possible permutations of evidence.

Mode of registration	Face to Face		Remote (online/telephone)	
Public Registration (<i>to be used as the primary source where possible</i>)	✓		✓	✓
Dealings with Government/ Membership /Trade/Operational	✓	✓ ✓ ✓	✓	
Third Party Corroboration				✓

Key ✓ = Must be provided. More than one tick indicates total number of that type of evidence to be provided.

Table 4-5: Minimum requirements for validation and verification of registrant organisation - Level Three

Note that a formal documented existing relationship with the RA may be used with at least one other piece of evidence only if the RA already has strong confidence in the identity of the registrant organisation. 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.

Mode of registration	Face to Face		Remote (online/telephone)	
Evidence of ID	✓ ✓		✓ ✓	
Evidence of affiliation with the organisation	✓		✓	
Evidence of authority to act for the organisation	✓		✓	
"Back Contact" with Registrant Organisation	✓		✓	

Key ✓ = Must be provided. More than one tick indicates total number of that type of evidence to be provided.

Table 4-6: Minimum requirements for validation and verification of registrant's representative - Level Three

4.4.2 Face to face

Registrant organisation

Documentary evidence that includes full formal name and full address of the organisation is required. This should always include official registration information where applicable (e.g. a registered company or registered charity), and include evidence of the identity of the supplier of the written authorisation to register (see below). An additional piece of evidence should also be added to demonstrate that the organisation is still in existence and active.

Registrant's representative

A personal statement giving details of identity and relationship with the company. The registrant's representative should supply two pieces of evidence identifying him/her as an individual, e.g. passport (as per authentication for individuals), and a document that identifies him in his/her capacity as a director/employee of the company.

Authority

Also needed is a document authorising the representative to undertake the enrolment. For a limited company, a copy of a board minute certified as true by a director and company secretary, or analogous evidence for other organisations. The identity of this manager/director must be included within the documentary evidence presented.

In addition, the Registration Authority should contact a director or a previously identified substitute at a published phone number to obtain additional verbal confirmation.

4.4.3 Remote Registration (with submission of documents)

The evidence must be of the same rigour as that presented at Level Two, and in addition there should be an additional document identifying the organisation and two pieces of ID for the Registrant's Representative, or two pieces of evidence associating him/her with the organisation.

4.4.4 Remote Registration (without submission of paper documents)

This may only be appropriate if the identity of the registrant's representatives, and their authority, can be established with a very high degree of assurance. It is recommended that in addition to the requirements at Level Two, a separate supporting request for registration should be obtained from a second director, whose identity should be verified in the same manner as the first. Alternatively, a single request, but from a director who has previously been verified to and registered with the RA in a personal capacity, can be used.

5. Problems and Issues with Registration

5.1 Wider application 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 may be appropriate for a financial organisation to insist the level 3 requirements are met.

5.2 Controlling interests in registrant organisations

For certain enrolment processes, such as opening a bank account, it may be necessary in some cases to "look behind"⁶ the identity of the Registrant Company or organisation to determine the controlling interest or the identity of individuals owning or running the organisation (e.g. in order to determine the underlying beneficial owners of funds). However, this is not the responsibility of the Registration Authority in the context of enrolment; 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. At enrolment, the responsibility of the Registration Authority is to establish the identity of the company or organisation, but not to look behind it.

5.3 Additional authentication by relying parties

This document sets out the requirements to be followed by Registration Authorities to authenticate organisations as a condition for issuing digital certificates. However, in many cases a relying party will also be in a position to undertake some additional verification from his/her own records when a customer presents with a credential. As noted previously, authentication is a cumulative process. As such, the relying party may gain additional assurance through undertaking his/her 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.

⁶ See for example '*Money Laundering Guidance Notes for The Financial Sector*', 2001 Edition, Joint Money Laundering Steering Group.

5.4 Storage and processing of information

Because 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.

© Crown Copyright 2003

The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as Crown copyright and the title of the document must be included when being reproduced as part of another publication or service.

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

