e-government

AUTHENTICATION FRAMEWORK

DECEMBER 2000

First published 2000

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

The Office of the e-Envoy

53 Parliament Street

London SW1A 2NG

email: seamless@citu.gsi.gov.uk

Website: www.citu.gov.uk

Designed and typeset by Format Information Design

Website: www.format-info.co.uk

Contents:

1 Introduction

Ownership and Maintenance

1. The Authentication Framework is one of a series developed as part of the Government's commitment, in the Modernising Government White Paper, to developing a corporate IT strategy for government. It has been prepared by the Office of the e-Envoy, part of the Cabinet Office, on behalf of the Information age Government champions.

2. This document builds on the IAG security policy as defined in the IAG Security Policy Framework document that sets out the IAG security requirements expressed in the Corporate Government IT Strategy. It specifically addresses those security requirements related to the provision of authentication services.

Who should read this Document?

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

Application, scope, and purpose

What are authentication services?

4. Authentication is the *process of verifying a claimed identity*. In the context of this paper, it includes:

- establishing that a given identity actually exists;
- establishing that a person or official of an organisation is the true holder of that identity;
- enabling identity holders to identify themselves for the purpose of carrying out a transaction via an electronic medium.

5. In the case of commercial transactions, the role of identity holders within their organisation may also need to be established.

6. Government and those it deals with have mutual obligations relating to authentication.

7. Government must:
- release personal or commercially sensitive information only against reliably verified identity;
- provide services and benefits only to those entitled to receive them;
- protect people against misuse of their identities.

8. Those dealing with government must be bound by declarations they have made and instructions they have given.

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

Scope of this Paper

10. This paper is concerned with the authentication of citizens and businesses seeking to access government services electronically. It applies in circumstances where government needs to have trust in the identity of those it is dealing with to ensure that there is no breach of privacy or confidentiality, or other harm. The Framework provides for those cases where anonymous or psuedonymous access is also acceptable. It is not applicable to transactions where government is simply receiving payments via electronic media in exchange for the provision of goods, services or information to consumers, for example where a government department wishes to sell goods over the Internet and sets up a web site accepting credit card payments. In these circumstances, normal commercial practice should be applied.

Organisations affected by this framework

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

12. For most electronic transactions, government will accept authentication provided by accredited third parties, which will register individuals and organisations and issue them with credentials enabling them to authenticate themselves in subsequent transactions.

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

- follow the guidance in this framework in order to allocate the transaction to an authentication level;
- adopt the profiles which will be prepared under this framework, and require any authentication service provider acting on their behalf to do so;
- note the advice on data protection contained in this framework, the more general work on this subject which forms part of the e-government strategy, and their obligations under data protection legislation; and
- ensure that they have considered all the risks set out in section 5 of this paper, and instituted adequate countermeasures.

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

Relationship to other Framework documents

15. The over-arching Information Age Government Security Framework document defines thirteen Service Control Objectives. The means of achieving these objectives are considered in more detail in other Framework documents.

16. The Authentication Framework document (this document) addresses the following objectives:
OS1 – Effective user identification and authentication
OS2 – Effective user registration
OS3 – Effective access control
OS4 – Effective user access management

17. The Trust Services Framework document addresses the following objectives:
OS5 – Non-repudiation
OS6 – Evidence of Receipt
OS7 – Trusted Commitment Service
OS9 – Integrity

18. The Confidentiality Services Framework document addresses the following objectives:
OS8 – Privacy and Confidentiality

19. Other framework documents address objectives OS10, OS11, OS12, and OS13.

20. In addition, the Privacy Framework will provide more detailed guidance on Data Protection, while the Call Centre Framework considers all these issues amongst others in that specific context.

2 Summary of Government's approach to authentication

Provision of trust services by third parties

1. Government will encourage the provision of authentication services by a variety of bodies, including local authorities and the private sector, and will seek to make use of these services wherever possible. Government welcomes the proposed T-Scheme for accreditation of trust service providers, currently being developed by the Alliance for Electronic Business (AEB), and will seek to work closely with the AEB to agree detailed standards for authentication services for government transactions.

Third party service delivery

2. The Modernising Government white paper makes clear government's intention to work in partnership with local authorities, the voluntary sector, and with third-party delivery channels such as the Post Office and private sector companies. Where third-party service providers are conducting transactions on government's behalf, they will be required to authenticate the citizens and businesses they deal with to the same standards as government itself would. Government will in turn accept transaction data from those service providers, who will certify that they have carried out the authentication transaction to the agreed standard.

Use of commercial technologies

3. Government will make use of normal commercial technologies and techniques for authentication. Authentication profiles applicable to government electronic service delivery are being developed in conjunction with industry. These include detailed security requirements.

General approach to authentication

4. For the purposes of IAG transactions, Government has defined levels of authentication that are appropriate to differing classes of transactions. In general, informal or lower value transactions will attract the lower levels of authentication requirements. Higher value, or legally significant transactions will attract more stringent authentication requirements.

5. At the lowest level, anonymous access to publicly available information is acceptable. At the highest level, face-to-face registration and the use of asymmetric key cryptographic is required. Departments should allocate each electronic service to an authentication level in accordance with the guidance contained in this framework. For each of these levels, government is defining a profile (set of requirements) setting out the mechanisms needed to achieve the required degree of confidence in the identity of the client. Separate profiles will be defined for business and citizen.

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

Definitions

7. We define here a number of terms that will be used in the following sections:

- 'Identity' means a set of attributes which together uniquely identify an individual (person, organisation or official of organisation).
- 'Identity holder' means the person, organisation or official of organisation to whom an identity genuinely relates.
- 'Registrant' means a person, organisation or official of an organisation seeking to establish their identity and obtain a credential from an issuer.
- The 'Registration Process' comprises: confirming the identity of the Registrant; collecting any user characteristics such as biometrics; issuing the Registrant with Credentials; and creating appropriate records in system reference files.
- 'Identity Issuer' means an organisation which, having established the validity of an identity, issues a credential to the identity holder, allowing their subsequent authentication
- 'Credential' means some object or information, issued or recorded by an issuer, used by an identity holder to authenticate themselves. A credential may consist of a combination of public information and of secret data, such as a PIN or private signing key.
- 'Register' means a register, maintained by an identity issuer, of identity holders who have been issued with credentials by that identity issuer.
- 'Client' means a person, organisation or official of an organisation seeking to carry out a transaction
- 'Relying party' means the party relying upon a credential to authenticate a client.
- 'Identification' is the way in which a client asserts a claimed identity to a system.
- 'Authentication' is the means by which that identity is verified.
- 'Hot list' means a list of credentials which have been withdrawn prior to their normal expiry date.

- 'Status responder' means a service which provides confirmation that a given credential remains valid, or conversely is no longer valid.
- 'Practice statement' means a statement, published by a service provider, setting out its practices in issuing and managing credentials.
- 'Unpublished data' means information which is likely to be known only to the identity holder and the identity issuer: for example, information about a previous transaction.

3 Authentication levels and Government transactions

1. This section describes the four authentication levels, and sets out guidelines for departments on allocating a given transaction to a given authentication level.

2. In allocating transactions to authentication levels, the relying party must consider direct and indirect consequences including financial issues, personal safety, undertakings made regarding the privacy of personal and commercial data and data protection legislation.

Level 0 - Informal transactions

3. Level 0 authentication is appropriate for IAG transactions where the communications between the parties are of an informal nature. In particular, misappropriation of identity would not result in:

- inconvenience to the identity holder; or
- risk to the identity holder's personal safety; or
- risk of the release of personal or commercially sensitive data to third parties; or
- risk of significant financial loss to any party; or
- risk to any party's standing or reputation; or
- risk of distress being caused to any party; and
- would not assist in the commission of or hinder the detection of serious crime.

4. Similarly, repudiation of the transaction would not result in:

- financial loss to the relying party; and
- would not assist in the commission of or hinder the detection of serious crime.

5. Examples of transactions that might merit level 0 authentication include:

- A citizen downloads publicly available information from a government web site.
- A citizen e-mails a government department with a request for general information and expects the material to be returned via e-mail.

Level 1 Personal transactions

6. Level 1 authentication is appropriate for IAG transactions where the relationships between the parties are of a personal nature but where mistaken identity would have a minor resource or nuisance impact on one or more of the involved parties (including the true identity holder). Such transactions would generally cover supply of information of a personal, but non-sensitive, nature. In particular, misappropriation of identity would not result in:

- major inconvenience to the identity holder; or
- risk to personal safety of the identity holder; or
- financial loss to the identity holder; or
- the release of personal or commercially sensitive data; or
- significant financial loss to the relying party; the identity holder or any third party; and
- would not assist in the commission of or hinder the detection of serious crime; and
- would not result in damage to the identity holder's reputation or standing; and
- would not result in significant distress being caused to any party.

7. Similarly, repudiation of the transaction would not result in:
   - significant financial loss to the relying party, and
   - would not assist in the commission of or hinder the detection of serious crime.

8. Examples of transactions that might merit level 1 authentication include:
   - A citizen apparently orders a low cost government publication over the Internet, but subsequently denies having done this. The impact is inconvenience and possible minor financial loss to the relying party, but there is no lasting impact on either party.

Level 2 Transactions with financial or statutory consequentials

9. Level 2 authentication is appropriate for IAG transactions between parties which are of an official nature and failure to undertake the transaction may be interpreted as a statutory infringement that may incur a penalty, or may involve the communication of information of a commercially or personally sensitive nature. In particular, misappropriation of identity might result in:
   - substantial inconvenience to the identity holder but would result in no risk to personal safety; or
   - the release of personally or commercially confidential data; or
   - significant financial loss to the relying party; the identity holder or a third party; or might
   - assist in the commission of; or hinder the detection of; serious crime; or
   - materially damage the identity holder's reputation or standing; or
   - cause significant distress to any party.

10. Similarly, repudiation of the transaction might result in:
    - significant financial loss to the relying party or a third party; or
    - might assist in the commission of or hinder the detection of serious crime.

11. Examples of transactions that might merit level 2 authentication include:
- A citizen files an income tax return electronically. The return should not be open to forgery, and details of the income tax assessment should not be released to an unauthorised third party.

Level 3 Transactions with substantial financial, statutory or safety consequentials

12. Level 3 authentication is appropriate for IAG transactions between parties which are of an official nature, and where mistaken identity may have significant financial impact or impact on the health or safety of installations or individuals. In addition to the consequences at level 2, misappropriation of identity might result in:
- risk to personal safety; or
- substantial financial loss to the relying party, the identity holder or a third party.

13. Similarly, in addition to the consequences at level 2, repudiation of the transaction might result in:
- substantial financial loss to the relying party or a third party.

14. In allocating transactions to trust levels, departments will need to consider the terms 'significant' and 'substantial' in the context of the parties likely to be affected. A significant loss to a pensioner might be a minor matter to a large company, for example.

15. Examples of transactions requiring level 3 authentication include:
- A citizen is issued a recall notice arising from participation in a health screening programme. Wrongly identifying the recipient could result in unnecessary treatment for one citizen, and an absence of treatment for another.

4 Authentication service provision

Level 0 authentication

1. An authentication service is categorised as Level 0 if no trust is put in the identities claimed by the transacting parties, other than a presumption of correct operation of the underlying technology.

2. For example, a client seeking public information from a government web site may access that information anonymously or psuedonymously. The web site will return the information to the requesting browser.

OS1 Effective user identification and authentication

3. No identification or authentication is required beyond provision of a return communications address if the client requires information to be sent back.

OS2 Effective user registration

4. No user registration is required.

OS3 Effective access control

5. Access control will only be permitted to publicly available information.

OS4 Effective user access management

6. No management of user access is required, beyond overall technological limits on access.

Level 1 authentication

OS1 Effective user identification and authentication

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

OS2 Effective user registration

8. Registration takes place largely on the basis of information supplied by the client, but some independent corroborative evidence is required.

OS3 Effective access control

9. Access will only be allowed to non-sensitive data pertaining to the identified client.

OS4 Effective user access management

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

Level 2 authentication

OS1 Effective user identification and authentication

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

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

OS2 Effective user registration

13. Registration uses some information supplied by the client, but with additional evidence that enables cross-checking of documents and/or third party corroboration.

OS3 Effective access control

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

OS4 Effective user access management

15. Validity of the credential must be time-bounded. In addition, the revocation status of the credential must be checked at the time of the transaction.

Level 3 authentication

OS1 Effective user identification and authentication

16. Users will identify themselves to the system by presentation of a digital certificate. This will preferably be held in a secure token, such as a smart card. Users will demonstrate their right to that credential through the use of a private key, and a password or biometric. The system will authenticate users based on the validity of public key / private key pairs, and on the validity of the credential.

OS2 Effective user registration

17. Registration requires the presentation of evidence of identity as for level two, plus additional evidence that may include demonstration of 'activity in the community'.

18. Face to face registration is required.

OS3 Effective access control

19. Access is permitted to all information pertaining to the client, provided it is governed by the permitted use of the credential.

OS4 Effective user access management

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

5 Risks and countermeasures

1. This section considers general risks pertaining to the registration process and those pertaining to subsequent misappropriation of identity. It does not consider risks and countermeasures concerning information held within the Government Network Domain or the Trusted Service Provider Domain. Nor does it consider risks relating to specific technologies: the technology-specific profiles will need to identify and counter specific risks to particular authentication technologies.

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

Risk	Possible countermeasures
R1) Fictitious Identity That a registrant will obtain a credential pertaining to a fictitious identity.	Possible countermeasures to ensure that an identity exists prior to the issue of credentials include: C1a) checking the details given against population or organisation registers; and/or C1b) examining original documents.
R2) False details That false information will be recorded against a genuine identity, and subsequently given credence.	Possible measures to ensure that attributes submitted as part of the registration process are accurate include: C2a) Checking the details given against population or organisation registers; and/or C2b) requiring the registrant to certify the accuracy of the information given; and/or C2c) requiring that a trustworthy person or organisation confirm the information given.
R3) Theft of identity token That an identity token containing a credential will be stolen from or while in transit to the identity holder, and will either itself be used by an impostor or will be used to obtain information about an identity for subsequent misuse.	Possible measures to reduce the risk of theft include: C3a) requiring that identity tokens are delivered using appropriate postal or courier services or issued in person only to the authenticated identity holder; and/or C3b) ensuring that identity tokens are usable only in conjunction with a PIN, password, biometric or other user verification mechanism. Any secret data intended for use in the verification process shall be delivered or issued separately from the token itself or stored securely within the token; and

Risk	Possible countermeasures
	C3c) ensuring that the minimum of public data is contained in accessible form on the token
R4) Identity theft That a genuine identity will be misappropriated at the time of registration.	Possible measures to ensure that credentials are issued only to the genuine identity holder include: C4a) examining original documents at the time of registration; and/or C4b) asking the registrant questions derived from unpublished information about the identity holder; and/or C4c) requiring that a trustworthy person or organisation vouch for the registrant; and/or C4d) contacting the supposed registrant at their registered address or telephone number; and/or C4e) sending the credential only to the registered address of the identity holder.
R5) Interception or revelation of secret authentication information That secret information (such as a PIN or private signing key) will be intercepted in transmission when the credential is used, will be accessed by a member of the relying party's staff, or will be revealed deliberately or inadvertently by the identity holder or another party.	Possible measures to reduce the risk of secret authentication information being intercepted or revealed include: C5a) ensuring that secret information is not transmitted at all, for example, by using a smart card to sign or encrypt information; or C5b) ensuring that secret information is transmitted only in encrypted form, or via an encrypted channel, or via an inherently secure communications link; and/or C5c) ensuring that secret information is not transmitted en bloc in clear; for example, in a call centre transaction the client may be asked to provide one character only from each of a series of secret numbers and/or phrases, and the operator should only have access to those single characters; and/or C5d) using dynamic rather than static information: in the case of authentication to a call centre, for example, asking the caller about a recent transaction is likely to be more reliable than asking about an account number or mother's maiden name, which may have been discovered by an impostor; and/or

Risk	Possible countermeasures
	C5e) placing a contractual requirement on the identity holder not to disclose secret authentication information.
R6) Retention of secret authentication information in untrusted terminal That secret information will be retained by an untrusted terminal (such as a home or office PC, PC in an Internet cafe or public kiosk). Such secret information may include for example private signing keys used to perform cryptographic functions within the terminal, and PIN numbers entered into a web-based form and subsequently held in cache.	Countermeasures against this risk will need to be technology-specific.
R7) Unauthorised use of authentication token That an authentication token will be used without the identity holder's authority.	Measures to protect against unauthorised use of an authentication token include: C7a) Requiring that authentication devices be protected by a system of identity holder verification, such as a password, PIN or biometric.
R8) Use of compromised credential That a credential will be used after it has been compromised.	Possible countermeasures against use of a compromised credential include: C8a) enabling and encouraging identity holders and relying parties to report suspected compromise to a continually available helpdesk service; and C8b) limiting the life of credentials to a fixed term; and C8c) enabling relying parties to check the validity of a credential at time of use, by reference to a stop list; and/or C8d) enabling relying parties to obtain positive verification of the validity of a credential at time of use, by means of an authorisation procedure.
R9) Use of credential after substantive change in circumstances	Possible measures to protect against the use of a credential after a substantive change in circumstances include: C9a) contractually obliging the identity holder to notify any change in circumstances; and

Risk	Possible countermeasures
	C9b) in the case of organisations, monitoring notifications of cessation of trading and stopping credentials; and C9c) requiring organisations to notify the identity issuer when a credential issued to one of their staff for business purposes should be stopped.
R10) Use of credential for unintended purposes That a credential will be used in connection with a transaction for which the issuer is not prepared to warrant it, because of the nature or value of the transaction.	Possible measures to reduce the risk of a credential being used for unintended purposes include: C10a) credentials being issued against practice statements; and C10b) credentials such as digital certificates incorporating any limitation as to use.
R11) Withdrawal of credential without due cause That a credential will be withdrawn due to a false or malicious report of change in circumstances, compromise of credential, etc	Possible measures to reduce the risk of, or inconvenience caused by, inappropriate withdrawal of a credential include: C11a) the ability to suspend rather than revoke a credential; and C11b) a continuously-available helpdesk service for identity holders; and C11c) the ability to replace a credential rapidly after withdrawal; and C11d) identity issuers having access to verification information to provide at least some assurance that the person reporting compromise or change in circumstances is genuine.
R12) Fraudulent use of credential That a credential holder will attempt to use their credential, either personally or through a third party, for transactions to which they are not entitled.	Possible measures to reduce the risk of unwarranted use of a credential include: C12a) contractually obliging the identity holder to use the credential for its intended purpose; C12b) using dynamic information to check that the credential is still held by the identity owner; C12c) using biometric data to ensure that the credential is held by the identity owner; C12d) ensuring that services provided are in accordance with limitations on use of the credential.

6 Implementation guidelines

Level 0

1. No specific implementation guidance is applicable to Level 0, which represents no greater intrinsic assurance of identity than is implied by the assumption of correct operation and use of the systems involved in the transaction.

Level 1

2. Authentication at level 1 is designed to prevent possible inconvenience to clients, and deter casual false or misappropriated identities.

3. Registration of a client should require a personal statement containing the full name of the applicant, their date of birth and current permanent address, with one piece of reputable documentary evidence or written corroboration from a trustworthy source. For business officials, this must be supplemented by evidence of the identity of the organisation, and of the official's capacity to act on behalf of that organisation.

4. Transaction time authentication may be undertaken using a username / password combination.

5. Management of user access should ensue that passwords are periodically changed, and that user accounts are disabled after a defined period of disuse, and/or after a specific date.

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

Levels 2 and 3

7. Authentication at levels 2 and 3 is designed to prevent consequences of a more serious nature.

8. Registration of a client requires the information to be provided for level 1, plus additional information that can be independently checked or corroborated. Face-to-face registration is preferred at level 3.

9. Transaction time authentication should be achieved through presentation of a digital certificate or similar credential, combined with a check that the client is in possession of a valid private key, password, or similar. For level 2 transactions, a username / password combination will be acceptable pending wider availability of public key infrastructures.

10. User access should be managed to ensure that credentials are checked for validity, that they have not expired, and that they have not been revoked. Limitations on the use of credentials should also be checked.

Further guidance

11. More detailed implementation guidance is available in the following documents:

Guidelines on the use of passwords (to be published)

Profile for authentication of individuals

Profile for authentication of limited companies, other corporate bodies and other organisations

The Authentication Concept of Operations (to be published)

General tScheme documentation.

7 Data protection

Data protection

1. There are potentially a number of data processors in any authentication scheme. These include the identity issuer, the relying party and any organisation verifying a customer's identity on behalf of the relying party at the time of transaction. All are bound by the requirements of the Data Protection Acts and by the Data Protection Principles.

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

- processed fairly and lawfully;
- obtained and processed for specified and lawful purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- held for no longer than necessary,
- processed in accordance with subject rights;
- kept secure; and
- kept within the European Economic Area, unless there are adequate safeguards.

3. Where personal data is processed on behalf of a data controller by a third party, the activities of the data processor must be governed by a written contract. In addition, providers of authentication services to government must comply with Annex C (Data Protection and retention policy) of Channels for Electronic Service Delivery: Draft Operating Policy, published by the Central IT Unit.

4. A number of specific points arise in respect of authentication. In particular:

- in order to comply with the seventh principle, adequate authentication is required to prevent unauthorised disclosure of personal data : indeed, for a given government service, there is a substantial likelihood that the authentication mechanism for the release of data in respect of that service will need to be stronger than that for submission of the data in the first place;
- data obtained for the purpose of verifying identity should not be used for secondary purposes;
- there must be transparency: it should be clear to the data subject why authentication information is being requested;
- whilst it may be necessary to retain for a reasonable period information given when identity is verified; for example for reasons of accountability and audit: the requirements of the fifth principle must be considered; and
- where a trust service provider authenticates an identity holder on behalf of one or more relying parties (as in the case of a 'portal' service), that trust service provider must pass on to each of the relying parties only that information which is relevant.

Appendix – The authentication lifecycle

Authentication lifecycle

1. Any authentication process will follow the broad lifecycle set out below, though not all steps will be undertaken in all circumstances. The steps to be taken will be defined in profiles, these are discussed in more detail in section 2

Register

2. Purpose:
- to ensure that the claimed identity actually exists;
- to ensure, so far as is possible, that the registrant is who they say they are (i.e. to prevent identity theft); and
- to ensure that the attributes associated with the identity are consistent, accurate and recorded in standard form.

3. Whilst a registration process normally precedes the issue of a credential for use in future transactions, the same process may be carried out on a one off basis in order to undertake a single transaction.

Validation: is this a valid identity?

4. Typically, and depending on the requirements of the specific profile, checks will be carried out as to whether:
- the postal address given actually exists (by reference to a postal address file);
- the individual or organisation is known to reside there (by reference to a population register, such as the electoral roll, or company register);
- the attributes given are consistent with available information; and
- in the case of an organisation, the registrant is known to be an official of that organisation.

Verification: is the registrant who they claim to be?

5. Typically, this will be established by examining whether:
- the registrant can produce original documents; and/or

- the registrant can answer questions derived from information about themselves/their organisation which is likely to be known only to the identity holder and the identity issuer; for example, information about a previous transaction; and/or
- a trustworthy person can vouch for them (as in a passport application); and/or
- a trustworthy organisation (such as an employer) can vouch for them; and/or
- the identity holder can be contacted at their registered address or telephone number.

Registration

- The issuing authority will record the steps it has undertaken to validate and authenticate identity, for audit purposes, and may
- convert the registration data into standard format (perhaps also carrying out some data cleansing by reference to a postal address file) and record it in its register.

Issue credential

6. Purpose:

- to issue a credential, or record details of an existing credential, so that the registrant may be authenticated when conducting transactions electronically.

7. (a) Issue of credentials

- Issue or agree PIN, passphrase, shared secrets, biometric template, token and/or private signing key.
- Store necessary verification information (such as a public key) in a directory, or store 'shared secret' verification information in an appropriate system.

Identify and authenticate at time of transaction

8. Purpose:

- to check that the credential presented has not expired or been withdrawn;
- to check that the credential is valid for the transaction in question; and
- to check that the credential is being used by the person or authorised signatory to whom it was issued.

Request client's identity

9. Obtain sufficient information about the client to identify them uniquely. (This might be from name and address, or a unique reference number issued by the relying party, and may be incorporated in the credential).

Verify client's identity

- Obtain authentication information (such as biometric information, passphrase, PIN number, token, or signed data) and check against stored data for supposed identity.
- Check that credential has not expired or been withdrawn, by reference to the issuer (for example checking a 'hot list', or obtaining positive confirmation of validity).
- Check that credential is suitable for transaction undertaken (i.e. that there is a sufficient level of trust and that the transaction is not excluded by the issuer by virtue of nature, value or risk).
- Preserve evidence of identity verification for audit purposes.
- Check validity of information given
- Check against known information that attributes given remain valid (for example, that the client has not changed address, died, left organisation etc).

Withdraw or suspend credential

10. Purpose:
- to withdraw and where necessary replace credentials in case of holder's death, resignation or dismissal, change of name, cessation of trading or other significant change of circumstance;
- to withdraw and replace stolen/compromised credentials;
- to suspend credentials where there is suspicion of compromise, theft or significant change of circumstances; and
- to withdraw credentials at the client's request.

Provide helpdesk service

11. An identity issuer should:
- Provide a continually available service to enable the identity holder to notify suspected loss or compromise of credentials, change of circumstances, etc.

Monitor published information

12. In addition, and particularly in respect of business credentials, an identity issuer may:
- monitor information used to issue credentials and proactively suspend credentials in the event of change of circumstances (such as cessation of trading).