Welcome

This is version 1.0 of the authentication framework for Information Age Government. It establishes a framework for authentication of online dealings with providers of public sector services.

This framework is endorsed by the Information Age Champions Group and will be an annex to the e-government strategy when it is published in March 2000. It will be kept under review by the Central IT Unit. A second edition of the framework will be published to coincide with the e-government strategy, together with more detailed guidelines on different trust levels. Proposals for additions and amendments to the guidelines may be made to authenticate@citu.gov.uk .

e-government strategy

Framework policy and guidelines for authenticating citizens and businesses to government

Executive Summary

1: Introduction
- Ownership and maintenance
- Who should read this document?
- Application, scope and purpose

2: The authentication lifecycle
- Key entities and entity relationships
- Authentication lifecycle

3: Summary of Government's approach to authentication
- Provision of trust services by third parties
- Third party service delivery
- Use of commercial technologies
- General approach to authentication

4: Trust levels and Government transactions

5: Risks and countermeasures

6: Data protection
- Data protection

7: Next Steps
- Development of Profiles
- Digital Signatures

Executive Summary

Effective government online and call centre services will require a widely accepted means for citizens and businesses to authenticate themselves for the purposes of those transactions. The essential characteristics of such a system of authentication are:

- an ability to inspire public confidence that personal data is properly protected, and to give assurance that the risk of impersonation is minimised;
- simplicity, transparency and economy to the user;
- common systems across government and the wider public sector;
- reduction of fraud and of wasteful duplication of effort.

The authentication framework policy and guidelines establish a common approach to authentication for government departments, agencies and the wider public sector. It is for implementation as new online and call centre services are developed.

The core requirements described in the guidelines are for:

- enrolment, the process by which a citizen or business is registered as entitled to authentication for a given level of services;
- means of authentication, which may utilise mechanisms such as PIN, password or digital signature, depending on the circumstances and level of authentication required;
- maintenance of registers of those enrolled;
- measures against theft and compromise of identity.

The framework policy does not assume or advocate the establishment of a single, national system of identification. Rather, it looks to the establishment of a range of authentication services by central and local government and the private sector, and for public sector bodies to use these. The framework policy sets out criteria for the management of information by those providing authentication services, including a reminder of the primacy of the data protection principles and the need for effective security.

The framework policy is supportive of the proposed T-Scheme for accreditation of trust service providers which is being developed by the Alliance for Electronic Business (AEB) in conjunction with the DTI.

At the core of the framework policy is the establishment of a set of four levels of authentication which can be used across the whole of Government. They are:

- Level 0: no authentication required;
- Level 1: authentication required to protect against minor inconvenience or loss;
- Level 2: authentication required to protect against significant inconvenience or loss;
- Level 3: authentication required to protect personal safety and/or to prevent substantial financial loss.

It will be for departments and agencies developing online and call centre services to determine which level of authentication is necessary for each service, taking into account the consequences, for both government and the citizen or business, of misidentification in respect of the transaction which is to be undertaken. The use of these levels of authentication across the public sector will familiarise citizens with the procedures and so develop increasing confidence in them. This will help to engender trust in online authentication and make its use more widespread. This is an essential step in the development of widespread use of e-commerce technologies in support of interactions with government.

1: Introduction

1.1: Ownership and maintenance

This framework is one of a series developed as part of the Government's commitment, in the Modernising Government White Paper, to developing an e-government strategy for government. It has been prepared by the Central IT Unit of the Cabinet Office on behalf of the Information age Government champions.

Other relevant frameworks include those relating to smart cards, security and data standards. The authoritative text of all these documents is published and maintained on the Information Age Government Champions' website, www.iagchampions.gov.uk

1.2: Who should read this document?

This document is aimed at the public sector, broadly defined, and at those delivering services on its behalf. It should be read by:

- information systems and business managers with a requirement to authenticate businesses and citizens carrying out electronic transactions by electronic means, including the telephone; and
- technical architects involved in implementing new forms of IT service delivery.

1.3: Application, scope and purpose

1.3.1: What is authentication?

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 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.

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

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

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.

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

Customers 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.

1.3.2: Scope of this paper

This paper is concerned with the authentication of citizens and businesses seeking to access government services electronically. It applies in circumstances where the 'real life' identity of the citizen or business is already held in connection with the service being accessed or where, in order to obtain the service, it is necessary for clients to give details of their real life identity. It is not applicable to circumstances in which

real life identity is not held or required in connection with the service being accessed. Nor is it 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 website accepting credit card payments. In these circumstances, normal commercial practice should be applied.

1.3.3: Organisations affected by this framework

This framework applies to all electronic transactions carried out by or on behalf of government where there is a need for authentication, subject to the provisos in 1.3.2 above. 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.

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.

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 a trust level, or to determine that verification of identity is not required;
- 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 7 of this paper, and instituted adequate countermeasures.

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

2: The authentication lifecycle

2.1: Key entities and entity relationships

A number of entities are involved in the authentication lifecycle: the key entities are as follows:

- '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.
- '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.
- '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.

The main relationships between these and other entities are illustrated in Figure 1.

Please download the diagram called fig1.gif from the web site [http://www.iagchampions.gov.uk/guidelines/authentication/images/fig1.gif].

Description: Figure showing how the entities interrelate. Refer to explanation in section 3.2
Figure 1: Main entities in the authentication lifecycle

2.2: Authentication lifecycle

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 3

2.2.1: Registration

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.

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.

2.2.1.1: Validation: is this a valid identity?

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.

2.2.1.2: Verification: is the registrant who they claim to be?

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.

2.2.1.3: 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.

2.2.2: Issue credential

Purpose:

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

(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.

2.2.3: Authentication at time of transaction

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.

2.2.3.1: Request client's identity

- 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).

2.2.3.2: 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.

2.2.3.3: 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).

2.2.4: Withdraw or suspend credential

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.

2.2.4.1: Provide helpdesk service

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.

2.2.4.2: Monitor published information

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).

3: Summary of Government's approach to authentication

3.1: Provision of trust services by third parties

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.

3.2: Third party service delivery

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. 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.

3.3: Use of commercial technologies

Government will make use of normal commercial technologies and techniques for authentication, although profiles will of necessity include detailed security requirements.

3.4: General approach to authentication

In summary, government's approach to authentication is as follows:

- A number of 'trust levels' are defined in Section 4 of this framework. These indicate the degree of confidence that will be required in the proof of identity submitted, before a given transaction may take place.
- Departments will allocate each electronic transaction to a trust level in accordance with guidance contained in this framework.
- For each trust level, government will define:A profile (set of requirements) setting out how identity holders are to be registered by identity issuers and how credentials are to be issued and managed throughout their lifecycle. One such profile will be required in respect of the authentication of businesses, and another in respect of members of the public, as the registration process in particular will differ significantly.
- One profile covering the issue or agreement of credentials, their subsequent management, and the means of achieving authentication at the time of transaction, in respect of each authentication technique or technology. It should be noted that some means of providing authentication may not be able to meet the higher trust levels.

This approach is illustrated in figure 2.

Please download the diagram called fig2.gif from the web site [http://www.iagchampions.gov.uk/guidelines/authentication/images/fig2.gif].

Description: Figure illustrating that each of the three levels of trust, from the lowest (level 1) to the highest (level 3) will have profiles relating to it for registration, validation and the lifecycle management of credentials. Separate profiles will be needed for businesses and consumers. Each level of trust will also have a profile relating to it for each type of authentication (digital signature, PIN, etc).
Figure 2: Profiles and levels of trust

In the first instance, government will seek to develop profiles for:

- authentication by means of digital certificates ; and
- authentication by means of PINs, passwords and/or memorable data, via the Internet and interactive

TV services;

- authentication by means of PINs, passwords and/or memorable data, via telephone call centres.

4: Trust levels and Government transactions
4.1:
This table sets out a number of trust levels, and guidelines for departments on allocating a given transaction to a given trust level.

In allocating transactions to trust 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.

Trust Level : 0 (No requirement for verification of identity)

- **Consequence of misuse of identity** : 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.

- **Consequence of repudiation of transaction by client** : 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.

Trust Level : 1

- **Consequence of misuse of identity** : Misappropriation of identity would not result in major inconvenience to the identity holder and would result in no risk to personal safety and no financial loss to the identity holder; andwould not result in the release of personal or commercially sensitive data data; and
- would not result in 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.

- **Consequence of repudiation of transaction by client** : 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.

Trust Level : 2

- **Consequence of misuse of identity** : Misappropriation of identity might result in substantial inconvenience to the identity holder but would result in no risk to personal safety; or
- might result in the release of personal or commercially confidential data; or
- might result in 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
- might materially damage the identity holder's reputation or standing; or
- might cause significant distress to any party.

- **Consequence of repudiation of transaction by client** : 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.

Trust Level : 3

- **Consequence of misuse of identity** : In addition to the consequences at level 2, misappropriation of identity might:result in risk to personal safety; or
- result in substantial financial loss to the relying party, the identity holder or a third party.

Consequence of repudiation of transaction by client : 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.

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.

5: Risks and countermeasures

5.1:

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.

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

Risk :
R1) Fictitious Identity

That a registrant will obtain a credential pertaining to a fictitious identity.

Possible countermeasures :
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.

Risk :
R2) False details

That false information will be recorded against a genuine identity, and subsequently given credence.

Possible countermeasures :
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.

Risk :
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 countermeasures :
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

C3c) ensuring that the minimum of public data is contained in accessible form on the token.

Risk :
R4) Identity theft

That a genuine identity will be misappropriated at the time of registration.

Possible countermeasures :
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.

Risk :
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 countermeasures :
Possible measures to reduce the risk of secret authentication information being intercepted or revealed include:

C5a) ensuring that secret information is transmitted only in encrypted form, or via an encrypted channel, or via an inherently secure communications link; and/or

C5b) 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

C5c) 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

C5d) placing a contractual requirement on the identity holder not to disclose secret authentication information.

Risk :

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.

Possible countermeasures :
Countermeasures against this risk will need to be technology-specific.

Risk :
R7) Unauthorised use of authentication token

That an authentication token will be used without the identity holder's authority.

Possible countermeasures :
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.

Risk :
R8) Use of compromised credential

That a credential will be used after it has been compromised.

Possible countermeasures :
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.

Risk :
R9) Use of credential after substantive change in circumstances

Possible countermeasures :
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

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.

Risk :
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 countermeasures :
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.

Risk :
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 countermeasures :
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.

6: Data protection

6.1: Data protection

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. Government has stated that it expects the Data Protection Act 1998 to be implemented from 1 March 2000, and that the 1984 Act will then be repealed in its entirety.

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.

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.

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 third party authenticates an identity holder on behalf of one or more relying parties (as in the case of a 'portal' service), that third party must pass on to each of the third parties only that information which is relevant.

7: Next Steps

7.1: Development of Profiles

Government will seek to develop profiles as described in section 3 under the auspices of the T-Scheme. In due course, these profiles will be published at www.iagchampions.gov.uk together with the authoritative text of version two of this document.

7.2: Digital Signatures

Digital signatures represent a particularly significant form of authentication. The cryptographic code which produces the signature is sufficiently difficult to forge that an extremely high degree of confidence can be placed in its origin. Within the provisions of the forthcoming Electronic Communications Bill, digital signatures will be legally valid signatures.

Digital signatures will play a central role in many of the profiles as described at Section 3, and assignment of digital signature standards to profiles will play a central part of the forthcoming liaison with the T-scheme. It is anticipated that Government will make full use of 3rd party Trust Service Providers in equipping citizens and businesses with digital signatures.

Government is also developing a Public Key Infrastructure for its own use (Cloud Cover: www.cesg.gov.uk/pubs/cloud). The Cloud Cover programme is intended to provide standards, policies and guidance for interoperability within Government; however, work is also in progress to maximise interoperability with Information Age Government services.