Office of the *e-Envoy*
Leading the drive to get the UK online

delivering

UK online

Trust Services

e-Government Strategy Policy Framework and
Guidelines

Version 3.0
September 2002

Contents

1. Introduction

1.1 Ownership and Maintenance

The e-Government trust services framework policy and guidelines document is one of a series developed as part of the Government's commitment, in the Modernising Government white paper[1], to developing a corporate IT strategy for government. It has been prepared by the Office of the e-Envoy, part of the Cabinet Office, on behalf of the e-Champions.

This document builds on the e-Government security policy[2] that sets out the e-Government security requirements. It specifically addresses those security requirements related to the provision of trust services to support access to e-Government services.

This version of the document incorporates comments received after a public consultation exercise.

1.2 Terminology

Trust Services are the means by which e-Government users (whether government users[3] or clients[4]) can make commitments (binding[5] or less formal) electronically, and if necessary, furnish the technical evidence to resolve any dispute. In the context of this paper, this includes:

a) Furnishing evidence that the apparent originator of an electronic transaction or communication must have been the real-world identity associated with the electronic identity. This contributes towards the security framework service control objective OS5 – **Non-repudiation**;

b) Furnishing evidence that the intended recipient of an electronic communication or second party to a transaction actually received the communication (if they did so). This contributes towards the security framework service control objective OS6 – **Evidence of receipt**;

c) Furnishing evidence that electronic payment instruments presented to a clearer for payment have been properly authorised for payment by the account holder. This contributes towards the security framework control objective OS7 – **Trusted commitment service**;

d) Furnishing evidence that the contents of an electronic communication or transaction as received by the recipient is the same as the communication sent by the originator and could not have been

---

1   *Modernising Government white paper.*

2   The latest version of *e-Government strategy framework policy and guidelines, security.* Available at http://www.e-envoy.gov.uk.

3   A government user is defined as a person or process that interacts with an e-Government service from a back office system or access system (in any capacity).

4   In the context of this document, a client denotes a person, an organisation, a representative of the person or organisation or a process.

5   A binding commitment is typically one where parties to the transaction are fulfilling statutory obligations or there is a requirement to commit resources.

modified, either deliberately or accidentally, *en route* to the recipient. This contributes towards the security framework security control objective OS9 – **Integrity**.

Depending on the circumstances, the evidence may be required to support informal agreements between parties to uncontroversial transactions, or it may be required to support increasingly formal circumstances such as government and clients meeting their obligations to each other or, ultimately, legal action to resolve disputed agreements. In addition, there may be a requirement to retain any evidence of performing the transaction. The business sponsor should establish what information should be retained by the parties in the transaction and inform the client. The business sponsor has responsibility for archiving information retained by government and for ensuring that clients understand their responsibilities.

Those organisations that provide the means to ensure confidence in e-Government services, such as Registration Authorities (RAs), credential issuers and Certification Authorities (CAs) are referred to as **trust service providers**.

The meaning ascribed to these and other specific terms in the document is provided in the glossary in the overarching security framework.

A list of abbreviations is also provided at annex A.

1.3   Who should read this document?

This document is aimed at those procuring and providing e-Government services. This includes Central Government Departments, non-departmental public sector bodies, Local Authorities and other local government bodies charged with the provision of e-Government services. It also encompasses regulatory bodies responsible for the proper audit and control of public assets and information.

In addition it includes the suppliers and service providers who wish to offer services themselves, provide and operate such systems on behalf of government or provide equipment in support of e-Government services.

It is also relevant to security authorities that may use this document to assess the suitability of offered solutions and accredit them for operational use.

1.4   Background

The e-Government registration and authentication framework document[6] addresses the means and measures required in order to ensure that a user (whether a client or a government user) has been correctly granted access to e-Government services. This is achieved by establishing an appropriate level of confidence in the real-world identity of a user requesting access rights, issuing credentials to be used in subsequent authentication, and validation of the credentials when the user interacts with an e-Government service (both as a client in a transaction and in the context of service provision).

In contrast, the trust services framework document is concerned with the *use* of the authenticated electronic identity of a user to establish mutual trust and commitment relationships *between* parties to an e-Government transaction. The trust services enable the parties to determine who originated the transaction, whether the transaction received matches the transaction sent, and whether the transaction was accepted by the recipient.

---

[6]   The latest version of *e-Government strategy framework policy and guidelines, registration and authentication*. Available at http://www.e-envoy.gov.uk

1.5   Objective

This document is intended to set out a number of levels of confidence in trust services used to support e-Government transactions.

Current guidance on the use of the security framework documents in the context of e-Government services is set out in the companion security architecture document[7].

1.6   Scope

This paper is concerned with the means by which clients can enter into commitments with respect to government services delivered electronically.

It is applicable where the correspondence passing between the parties may be cited in support of binding commitments made by that communication. The framework is also applicable in less formal situations where failure to meet informal obligations may incur some cost or inconvenience.

This policy is intended only to cover commitments made between clients and government in the context of e-Government services. This includes communications between access and back office systems that are necessary to provide an end-to-end service. It does not apply to government-to-government transactions that are not concerned with e-Government service provision.

1.7   Organisations affected by this document

This framework applies to all electronic transactions carried out by or on behalf of government where the transactions result in commitments between government and clients. It is intended to ensure that all government bodies, and organisations providing services on their behalf, provide trust services in a consistent manner when providing services electronically.

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

a)   follow the guidance in this framework in order to allocate the transaction to a trust service level;

b)   follow the guidance in this framework to deliver appropriate trust service processes and functionality for the assigned level;

c)   note the requirements of the e-Government strategy and security framework, and more general requirements with respect to the legal enforceability of electronic transactions; and

d)   ensure that they have considered all of the risks set out in section 4 of this paper and instituted appropriate countermeasures.

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.

---

[7]   The latest version of *e-Government strategy: security architecture*. Available at http://www.e-envoy.gov.uk

1.8   Relationship to other framework documents

The over-arching e-Government security policy framework document defines the following service control objectives. The means of achieving these objectives are considered in detail in this and other framework documents.

The documents form a complete set and it is strongly suggested that they should be read together. The overarching security policy framework document also provides guidance on how the documents should be used for the process of service security requirements specification and accreditation.

The e-Government registration and authentication framework document addresses the following objectives:

a)   OS1 – Effective user identification and authentication;

b)   OS2 – Effective user registration;

c)   OS3 – Effective access control;

d)   OS4 – Effective user access management.

The trust services framework document (this document) addresses the following objectives:

a)   OS5 – Non-repudiation;

b)   OS6 – Evidence of receipt;

c)   OS7 – Trusted commitment service;

d)   OS9 – Integrity.

The confidentiality framework document[8] addresses the following objective:

a)   OS8 – Privacy and confidentiality.

The business services framework document[9] addresses the following objectives:

a)   OS10 – Service availability;

b)   OS11 – Information availability;

c)   OS13 – Effective audit and accounting.

The network defence framework document[10] addresses the following objective:

a)   OS12 – Service protection.

---

[8]   The latest version of *e-Government strategy framework policy and guidelines, confidentiality*. Available at http://www.e-envoy.gov.uk

[9]   The latest version of *e-Government strategy framework policy and guidelines, business services*. Available at http://www.e-envoy.gov.uk

[10]   The latest version of *e-Government strategy framework policy and guidelines, network defence*. Available at http://www.e-envoy.gov.uk

The assurance framework[11] document addresses the means by which trust in the implementation of security elements can be assured.

1.9   Availability of advice

In the first instance, advice on the application of the trust services framework may be obtained from the Office of the e-Envoy[12].

CESG[13] is the national technical authority on information security and may be consulted for further advice and assistance on technologies, measures and products to meet these requirements.

---

[11]   The latest version of *e-Government strategy framework policy and guidelines, assurance*. Available at http://www.e-envoy.gov.uk.

[12]   http://www.e-envoy.gov.uk.

[13]   Telephone 01242 237323 or via http://www.cesg.gov.uk.

2. Summary of Government's approach to trust services

2.1　Introduction

This section sets out the approach to the provision of all or part of e-Government services by third parties, including obligations on third parties for provision of trust services.

An overarching operations concept for a client engaging in e-Government transactions in the context of the Government Gateway, and with the current limitations on the use of PKI, is given in the Security Architecture

2.2　Third party participation in provision of e-Government services

2.2.1　Provision of trust services by third parties

Government will encourage the provision of trust services by a variety of bodies, including local authorities and the private sector, and will seek to make use of these services wherever possible. Government welcomes the *tScheme* for accreditation of trust service providers, which has been set up by the Alliance for Electronic Business (AEB), and will seek to work closely with the AEB and other relevant bodies to agree detailed standards for trust services for government transactions.

Any third party providing trust services to support e-Government transactions should normally be approved under a scheme recognised by the UK government such as *tScheme*.

2.2.2　Third party service delivery

The Modernising Government white paper makes clear the government's intention to work in partnership with local authorities, the voluntary sector, and with third-party delivery channels such as the Post Office and private sector companies. Where third-party service providers are conducting transactions on the government's behalf, they will be required to secure the transactions to the same standards as government itself would. Government will in turn accept transaction data from those delivery channels, which will certify that they have carried out the transaction to the agreed standard. Third party delivery channels working on behalf of government may wish to provide their own trust services or use those provided by a different third party.

2.2.3　Use of commercial technologies

Government will make use of commercial technologies and techniques for e-Government trust services. Where necessary, government will work with commercial suppliers to ensure that their products are compatible with government security requirements. It is only through such compatibility, and the possibility of cross-certification, that the (technical) concept of trust may be irrefutably transferred.

The use of system components that have been formally certified under the ITSEC and/or Common Criteria schemes is encouraged. However, there will be no general requirement for systems to undergo ITSEC or Common Criteria evaluations. The process for assurance of systems hosting e-Government services is described in the e-Government assurance framework.

It is considered acceptable to require a client to install a standard commercial security product in order to access e-Government services, for example a web browser with an up-to-date version of the Secure Sockets Layer (SSL) protocol. However, the requirement of client-installed custom software to access e-Government services should be avoided.

Government will make best efforts to ensure that services are accessible from a wide range of platforms (*eg* Personal Computers (PCs), kiosks *etc*), but cannot guarantee to include all. In those circumstances, electronic services may be unavailable.

2.3   General approach to trust services

For the purposes of e-Government transactions, government has defined levels of trust services that are appropriate to differing classes of transaction. In general, informal or lower value transactions will attract the lower levels of trust service requirements. Higher value or legally significant transactions will attract more stringent trust service requirements.

A trust service level should be assigned to a transaction independently of levels assigned in respect of registration, authentication, confidentiality, business services and network defence. For example, there is no requirement that the trust service level assigned to an e-Government transaction is the same as that for registration.

However, since trust services rely on the use of specific authentication technologies to provide evidence of commitments entered into in e-Government transactions, it is likely that the authentication level will be equivalent to or higher than the trust services level. The level of trust in a transaction is unlikely to be greater than that placed in the electronic identities of the parties.

If a commitment is also bound to a real-world identity disclosed in a transaction, then the registration level is also likely to be greater than or equal to the trust services level.

It should be noted that the above relations between trust, registration and authentication levels are merely guidelines. Service providers must review the levels assigned as a coherent set and ensure that all necessary functionality is provided. For example, if there is no strong binding between the registration and authentication processes, one can only make tentative assumptions about the real-world identity of the user. In addition, if PKI is used, the strongest non-repudiation is achieved by the use of hardware tokens, which has consequences for the authentication process.

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

Requirements as to the length of time for which evidence should be retained will be determined for each class of transaction by the business sponsor. Any responsibility on the client for retention of evidence must be clearly communicated.

Consideration needs to be given to the integrity and confidentiality of audit and accounting logs to support evidence retained. This aspect is covered more generally in the business services framework document[14].

Service providers must be aware that the degradation of encryption technology over time will have consequences for the strength of evidence retained as, for example, it may be easier to forge signatures and determine private keys.

Government will provide its own certification authorities for use in the public sector and may require some transactions to be certified by its own Certification Authority (CA) or the government root CA used to complete trust relationships. At the current stage, commercial CAs cannot fall under or be cross-certified by the HMG root.

This document concentrates on non-repudiation, evidence of receipt, integrity and trusted commitment services. Other trust services (for example time stamping and record management services *etc*) may also be required but are outside the scope of this document and need to be considered on a case-by-case basis as part of the development of the security concept and security policy.

---

[14] The latest version of *e-Government strategy framework policy and guidelines, business services*. Available at http://www.e-envoy.gov.uk

3. Trust service levels in government transactions

3.1 Introduction

This section defines the four trust service levels, which represent degrees of impact of failure to keep commitments made (*eg* through repudiation, misdirection or loss of integrity). The levels are layered according to the severity of consequences that might arise.

It also gives examples of transactions and service provision guidelines under this scheme. Examples of transactions that might merit particular trust service levels are not intended to be definitive.

In allocating transactions to trust service levels, the relying party must consider all the direct and indirect consequences laid out in the definitions of the levels. In addition, departments will need to consider the terms 'minor', 'significant' and 'substantial' in the context of the parties likely to be affected. A significant financial loss to an individual might, for example, be a minor matter to a large company.

Departments must determine the level implied for each consequence and allocate the highest of these to the transaction. For example, if failure of the transaction by repudiation or loss of integrity might result in risk to the client's personal safety, then the transaction must be allocated to trust service level 3, even if potential financial loss or other consequences are minimal.

Service providers must also consider the level assigned in terms of risks to the service as a whole, cost of implementation, practicality and overall business benefit. They may, in exceptional circumstances, be granted a waiver on adherence to this framework, subject to review during the assurance process.

Service provision guidelines are given in association with each level. These are related to service control objectives OS5 ('Non-repudiation'), OS6 ('Evidence of receipt'), OS7 ('Trusted commitment service') and OS9 ('Integrity').

Attention must be paid to the individual processes that make up the transaction. In some cases it will be sufficient to provide a trust service for transaction delivery and in others the transaction extends to the back-office system and the trust service will be needed to confirm processing (since, strictly, the transaction only ends with the delivery of goods or services). In cases where a portal service fragments a transaction to pass it to more than one department or process, service providers will need to determine the appropriate points at which to provide trust services such as acknowledgement of receipt or non-repudiation.

In addition, service providers must ensure that it is possible to provide a persistent binding between security information and transaction material regardless of the extent to which the information is split up for processing.

The service provision guidelines given here refer mainly to government users. Consideration must also be given to measures that may be used in the client network domain. Service providers should provide advice to clients on how they can safeguard evidence of commitments entered into with e-Government services, and make clear to them their obligations for retention of this information.

3.2   Level 0 – minimal damage

3.2.1   Definition

Level 0 trust services are appropriate for e-Government transactions in which **minimal damage** might arise from failure to keep any commitments made. Such transactions would generally cover supply of information of a non-sensitive or non-personal nature and informal advice and guidance of a general nature. In particular, failure of the transaction (by repudiation, misdirection, loss of integrity *etc*) at level 0 might result in at most:

> minimal inconvenience to any party; or

> no risk to any party's personal safety; or

> no release of personally or commercially sensitive data to third parties; or

> minimal financial loss[15] to any party; or

> no damage to any party's standing or reputation; or

> no distress being caused to any party; or

> no assistance in the commission of or hindrance to the detection of serious crime.

3.2.2   Examples

Examples of transactions that might merit level 0 trust services include:

a)   A client reads or downloads publicly available information from a government website. Loss of integrity of the information might cause minimal inconvenience to the client and no risk to safety or other adverse effects.

b)   A client emails a government department with a request for general information and expects the material to be returned via email. Misdirection of the communication might result in minimal inconvenience but no distress, damage to reputation or other consequences.

3.2.3   Service provision

A trust service is categorised as level 0 if the trust is obtained by the use of standard communication components and protocols with no specific trust enhancements other than a presumption of correct operation and use of the systems upon which the service is hosted. Business sponsors must be aware of, and accept the risks associated with, reliance upon an untrusted platform.

The content of, and participants in, a transaction could be identified in the relevant fields of the protocol. For example, an email will have an originator field and a message content and the recipient of the email may choose to act upon that information though the binding between the actual originator of the message and the purported originator is weak or absent.

---

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

OS5: Non-repudiation

The originator identity (electronic, or real-world) and, optionally, a transaction reference number may be used to provide simple assurance that a transaction or an object originated from a purported source. No additional mechanisms over and above the normal service elements are provided. For example, email identified as originating from user@dept.gsi.gov.uk is assumed to originate from "user"; for web services, the page presented by http://www.dept.gov.uk/ can be assumed to originate from that department.

OS6: Evidence of receipt

Existing service mechanisms are used to provide simple assurance that an object has been received by the recipient[16]. No additional mechanisms over and above the normal service elements of the system are provided. For example, an email reply stating that a transaction has been received or the display of a web page acknowledging a request is sufficient.

OS7: Trusted commitment service

Trusted commitment services require that the commitment information provided be protected with an appropriate level of non-repudiation, proof-of-receipt and integrity.

OS9: Integrity

Existing protocols are used to provide simple protection for data in transit. The user may be able to determine where modification has occurred, *eg* document format errors or incomplete web pages.

3.3   Level 1 – minor damage

3.3.1   Definition

Level 1 trust services are appropriate for e-Government transactions in which **minor damage** might arise from failure to keep any commitments made. Such transactions would generally cover supply of information of a personal nature and informal agreements to some future action. In particular, failure of the transaction (by repudiation, misdirection, loss of integrity *etc*) at level 1 might result in at most:

a)   minor inconvenience to any party; or

b)   no risk to any party's personal safety; or

c)   no release of personally or commercially sensitive data to third parties; or

d)   minor financial loss to any party; or

e)   minor damage to any party's standing or reputation; or

f)   minor distress being caused to any party; or

g)   no assistance in the commission of or hindrance to the detection of serious crime.

3.3.2   Examples

Examples of transactions that might merit level 1 trust services include:

---

16   The measures here of course only give evidence that the transaction has been received by the recipients communications equipment or electronic address. If evidence is required that a specified real-world identity has received the transaction, a higher level of trust should be used for which the receipt is bound to the recipient identity.

a) A client arranges a meeting with a government official by email. The impact of failure is inconvenience and lost time, possibly minor financial loss, but no lasting impact on either party.

b) A client purchases a low cost government publication over the Internet. The impact of failure is inconvenience and possibly recovering or refunding incorrect payments.

c) A client requests general or case specific information from a government department which is needed to meet some obligation to a third party and which the department has a published commitment to supply promptly. The consequences of failure to obtain the information are inconvenience or delay but are not business critical.

3.3.3   Service provision

A system hosting level 1 trust services should be based upon a platform where some attention has been given to its intrinsic trust vulnerabilities and an informed decision taken as to which risks are acceptable.

Measures that can be adopted to improve the trustworthiness of systems include ensuring that the system configuration is under proper control and unauthorised entities cannot gain access and modify the important configuration data such as Domain Name Server (DNS) databases and the network addressing and routing structures. Where such configuration is outside the scope of the system (*eg* the Internet) then the vulnerabilities should be understood by system management and the risks accepted.

Level 1 trust services will be provided by standard communication systems and protocols where more control over the provision of service can be achieved and/or additional informal or procedural measures are adopted. Level 1 is intended to encompass systems that implement additional security mechanisms providing a degree of confidence in the overall system, but where the security mechanisms implemented are less than fully secure.

Systems implementing security mechanisms that do not provide a strong and persistent binding between a transaction and corresponding security information may also be considered level 1.

Level 1 provides no more than a basic assurance in the provision of a service. Examples of level 1 based systems include: a system utilising a simple password based scheme or a system using a transport layer security mechanism such as the emerging Transport Layer Security Protocol (TLS) without close control of the certificate management.

OS5: Non-repudiation
Essentially as for level 0 with some review of the system configuration to ensure that the standard services and protocols are not obviously vulnerable to attack.

Additional degrees of trust may be achievable by the use of informal technical measures such as the agreement of passwords via out-of-band routes (for example printed correspondence). These passwords may then be used with simple encryption or signing tools to demonstrate possession of the password to correspondents. Another simple technique to reduce the scope for later repudiation is to provide the client at intervals with a list of transactions to date.

It is important that expert guidance be sought when setting up such schemes, as the additional trust achieved is often illusory unless the scheme is carefully constructed. Such schemes are rarely foolproof, it is therefore important that the limits of such schemes are understood and accepted by parties to the transaction. However, these methods may support a useful extra degree of trust in specific cases and provide the client with greater confidence.

Appropriate audit log files should be kept, showing transaction times and records of system operation.

OS6: Evidence of receipt
Evidence of receipt is typically achieved by returning evidence of possession of the message to the originator under a non-repudiation service. Close attention to system configuration possibly supported by informal mechanisms may be used to achieve this in line with the level 1 non-repudiation approach.

OS7: Trusted commitment service
Trusted commitment services require that the commitment information provided be protected with an appropriate level of non-repudiation, proof-of-receipt and integrity.

OS9: Integrity
Message integrity is often a feature of standard communications protocols. The use of checksums provides adequate protection against accidental corruption of a message. If greater assurance in the message integrity is required, informal mechanisms involving passwords and Personal Identification Numbers (PINs) may be adopted.

3.4   Level 2 – significant damage

3.4.1   Definition
Level 2 trust services are appropriate for e-Government transactions in which **significant damage** might arise from failure to keep any commitments made. This level would cover transactions of an official nature in which failure to complete the transaction may be interpreted as a statutory infringement that may incur a penalty, or which may have a significant impact on a third party. In particular, failure of the transaction (by repudiation, misdirection, loss of integrity *etc*) at level 2 might result in at most:

significant inconvenience to any party; or

no risk to any party's personal safety; or

the release of personally or commercially sensitive data to third parties; or

significant financial loss to any party; or

significant damage to any party's standing or reputation; or

significant distress being caused to any party; or

assistance in the commission of or hindrance to the detection of serious crime.

3.4.2   Examples
Example transactions that might merit level 2 trust services include:

a)   A client files an income tax return electronically. The client may subsequently seek to deny responsibility for the contents of the return claiming forgery or interference. This might result in significant inconvenience, distress, financial loss and / or damage to reputation of the involved parties.

b)   A client pays a fixed penalty fine. Government may deny receipt thus incurring additional penalty charges and significant financial loss to the client.

c) A business is seeking to fulfil an order that requires export licence or credit guarantee. The government department may fail to respond claiming it never received the request and the order is lost. This might result in significant damage to the business.

3.4.3   Service provision

Level 2 trust services require a persistent binding between transactions and security information supporting the trust service. A digital signature using public key cryptographic techniques is the current mechanism of choice to provide the binding.

Level 2 trust services should, where possible, be provided by commercial digital signature products. Conformance with government recommendations for the implementation of PKI systems is recommended, but not required.

However, other mechanisms, based for example on username and password, may be acceptable (though strongly deprecated owing to the significant degradation of the security provided) while widespread PKIs are unavailable. Service providers must clearly document the associated reduction in trust and explicitly accept the additional risks of such methods or assign the transaction to a lower level.

OS5: Non-repudiation

A transaction or a digest of the transaction, signed by the originator, should be used to provide Level 2 evidence of origin. The signature must be verified by the recipient of the transaction, or by a third party. Ownership of any public keys must be verified by a recognised entity, which may be the recipient or some other party.

Appropriate audit log files should be kept, showing transaction times and records of system operation. At this level, it may be appropriate to include a means for providing a record of the transaction as seen by the client.

OS6: Evidence of receipt

A response demonstrating receipt of a transaction must be returned to the transaction originator. The returned response must be protected by an integrity service and a non-repudiation service. The response may be generated manually or automatically. A level 2 evidence of receipt service may be provided by a system that can provide a combination of a level 2 non-repudiation and level 2 integrity services.

OS7: Trusted commitment service

Trusted commitment services require that the commitment information provided be protected with an appropriate level of non-repudiation, proof-of-receipt and integrity.

OS9: Integrity

A transaction or a digest of the transaction, signed with the private signature key of the originator, will provide level 2 evidence of integrity. The signature must be verified by the recipient of the transaction. Modifications or errors in the signed object, whether accidental or deliberate, will cause verification of the signature to fail.

3.5   Level 3 – substantial damage

3.5.1   Definition

Level 3 trust services are appropriate for e-Government transactions in which **substantial damage** might arise from failure to keep any commitments made. This level would cover transactions of an official nature in which failure to complete the transaction might have a substantial financial impact

(which might not be recoverable), or impact on the health or safety of installations or individuals. Such transactions may be attractive to criminal exploitation leading to a substantial risk of fraud or criminal damage. In particular, failure of the transaction (by repudiation, misdirection, loss of integrity *etc*) at level 3 might result in at most:

> substantial inconvenience to any party; or

> risk to any party's personal safety; or

> the release of personally or commercially sensitive data to third parties; or

> substantial financial loss to any party; or

> substantial damage to any party's standing or reputation; or

> substantial distress being caused to any party; or

> assistance in the commission of or hindrance to the detection of serious crime.

3.5.2 Examples
Example transactions that might merit level 3 trust services include:

a) A client is issued a recall notice arising from participation in a health-screening programme. A failure to complete the transaction might prevent or delay treatment for the condition detected, causing risk to the client's health and substantial distress among other consequences.

b) An organisation files a fraudulent Value Added Tax (VAT) return electronically and, upon being challenged, may deny submitting the return. Criminal activities may not be provable without adequate trust in the transaction.

c) A laboratory service providing clinical tests may file the results electronically to speed up response to the results. The consequence of wrongly attributing the results to the patients may be serious and must be minimised, it must be clear where such an incorrect attribution arose.

d) A client receives results of medical testing electronically. The client needs to be assured that the results are indeed from the service provider and could not have been altered in transit. Any loss of integrity might cause significant distress to the client and damage to the reputation of the service provider.

3.5.3 Service provision
Level 3 trust services are intended to be provided by commercial products utilising public key technology to provide digital signatures. Compliance with Government recommendations for the implementation of PKIs is expected. Evaluation by a recognised independent body, e.g. ITSEC or Common Criteria is recommended.

OS5: Non-repudiation
As for level 2, with the mechanism used to identify ownership of the public key provided by approved mechanisms. In addition, products and systems must provide appropriate protection for private keys and use standardised formats and protocols.

Appropriate audit log files should be kept, showing transaction times and records of system operation. At this level, it may be appropriate to include a means for providing a record of the transaction as seen by the client.

OS6: Evidence of receipt
As for level 2, with the non-repudiation on the provision of the receipt protected with level 3 non-repudiation and level 3 integrity services.

OS7: Trusted commitment service
Trusted commitment services require that the commitment information provided be protected with an appropriate level of non-repudiation, proof-of-receipt and integrity.

OS9: Integrity
As for level 2 integrity services except that a PKI approach is assumed.

3.6   Policy on use of digital certificates for trust services

Trust service levels 2[17] and 3 require the use of a PKI and digital signatures.

A principal concept behind the use of digital signatures is that the binding between the public key and the electronic/real-world identity of the owner of that key can also be protected using a digital signature. The protecting signature is typically that of a CA.

A CA may have a certificate that binds its own real-world identity to its own public key. This certificate may be issued by the CA itself (a self-signed certificate) or by another CA that is prepared to vouch for the real-world identity of the first CA and to vouch for the binding between the CA's real-world identity and the CA's public key.

In this way, certificates may be chained, *ie* the signature on one certificate is used to verify the public key used to sign another object (which can be a transaction or another certificate). A succession of certificates chained in this manner is termed a certification path. A mechanism is required by which trust can be placed in the initial certificate in the path.

The following table sets out the functional areas that need to be considered when implementing a secure system together with the corresponding requirements for trust service levels[18].

Functional Area	Requirements on Trust Levels
Security of the private key The security of public key systems rests on the measures used to protect private keys. Verified recognised mechanisms must be used to protect the private keys of both clients and certification authorities.	Level 2: protection of the private key using a recognised and approved software or hardware token. Level 3: protection of the private key using recognised, cryptographically assessed and approved software or hardware token. (There are a number of schemes that would be able to assess the security of a particular device, such as FIPS-140, Common Criteria, and CAPS (CESG Assisted Products Scheme) to name but a few).
Accreditation The service offered should be approved under a recognised accreditation scheme.	The service shall be approved under *tScheme* (or equivalent)

---

[17]   Username/password measures are only allowed at level 2 for a limited time and are strongly deprecated owing to the significant degradation of the security provided.

[18]   Requirements are only stated for trust service levels 2 and 3, since it is only for these levels that a PKI is required.

4. Risks and Countermeasures

The risks and countermeasures required to implement trust services are similar to those pertaining to the registration and authentication processes. Those risks particularly applicable to trust services are repeated below.

Risk	Possible Countermeasures
R1) Identity related risks That a client or service provider participates in a transaction with an entity not authorised to do so. This may occur through registration of a false real-world identity or misappropriation of an electronic or real-world identity. Further details are given in the registration and authentication framework.	Entities (clients and government users) will be required to undergo registration and authentication in order to access e-Government services. The methods for implementing these processes are given in the registration and authentication framework.
R2) Theft of access token That an access token containing a credential will be stolen from or while in transit to the user, and will itself be used by an impostor, or will be used to obtain information about a user for subsequent misuse.	Possible measures to reduce the risk of theft include: C2a) requiring that access tokens are delivered using appropriate postal or courier services or issued in person only to the registered user; C2b) ensuring that access tokens are usable only in conjunction with a PIN, password, biometric or other user verification mechanism. Any secret data for use in the verification process shall be delivered or issued separately from the token itself or stored securely within the token; C2c) ensuring that the minimum of public data is contained in accessible form on the token.
R3) 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 government user or will be revealed deliberately or inadvertently by the client or another party.	Possible measures to reduce the risk of secret authentication information being intercepted or revealed include: C3a) ensuring that secret information is not transmitted at all, for example, by using a smart card (for which the private key never leaves the token) to sign or encrypt information; C3b) ensuring that secret information is transmitted only in encrypted form, or via an encrypted channel, or via an inherently secure communications link; C3c) 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; C3d) using dynamic rather than static information; in the case of verification of identity 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; C3e) placing a contractual requirement on the client not to disclose secret authentication information.

Risk	Possible Countermeasures
R4) 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 café or public kiosk). Such secret information may include for example private signing keys used to perform cryptographic functions within the terminal, and PIN numbers entered into a web–based form and subsequently held in cache.	Countermeasures against this risk will need to be technology–specific but could include: C4a) ensuring that secrets are not stored in an untrusted environment, rather they are kept wholly within a trusted token such as a smart card programmed to perform the signing act; C4b) ensuring that secrets are properly controlled and positively purged when no longer required.
R5) Use of compromised credential That a credential will be used after it has been compromised.	Possible countermeasures against use of a compromised credential include: C5a) enabling and encouraging clients and relying parties to report suspected compromise to a continually available helpdesk service; C5b) limiting the life of credentials to a fixed term; C5c) enabling relying parties to check the validity of a credential at time of use, by reference to a credential revocation list; C5d) enabling relying parties to obtain positive verification of the validity of a credential at time of use, by means of an authorisation procedure.
R6) Use of credential after substantive change in circumstances That a credential will be used when a change in circumstances means that the credential would not normally have been issued.	Possible measures to protect against use of a credential after a substantive change in circumstances include: C6a) contractually obliging the client to notify any change in circumstances; C6b) in the case of organisations, monitoring notifications of cessation of trading and stopping credentials; C6c) requiring organisations to notify the registration authority when a credential issued to one of their staff for business purposes should be stopped.
R7) 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: C7a) credentials being issued against practice statements; C7b) credentials such as digital certificates incorporating limitations as to use.

A   Abbreviations

CA   Certification Authority

CRL   Certificate Revocation List

DNS   Domain Name Server

PC   Personal Computer

PIN   Personal Identification Number

PKI   Public Key Infrastructure

RA   Registration Authority

SSL   Secure Sockets Layer

TLS   Transport Layer Security

VAT   Value Added Tax