



Office of the *e-Envoy*

Leading the drive to get the UK online

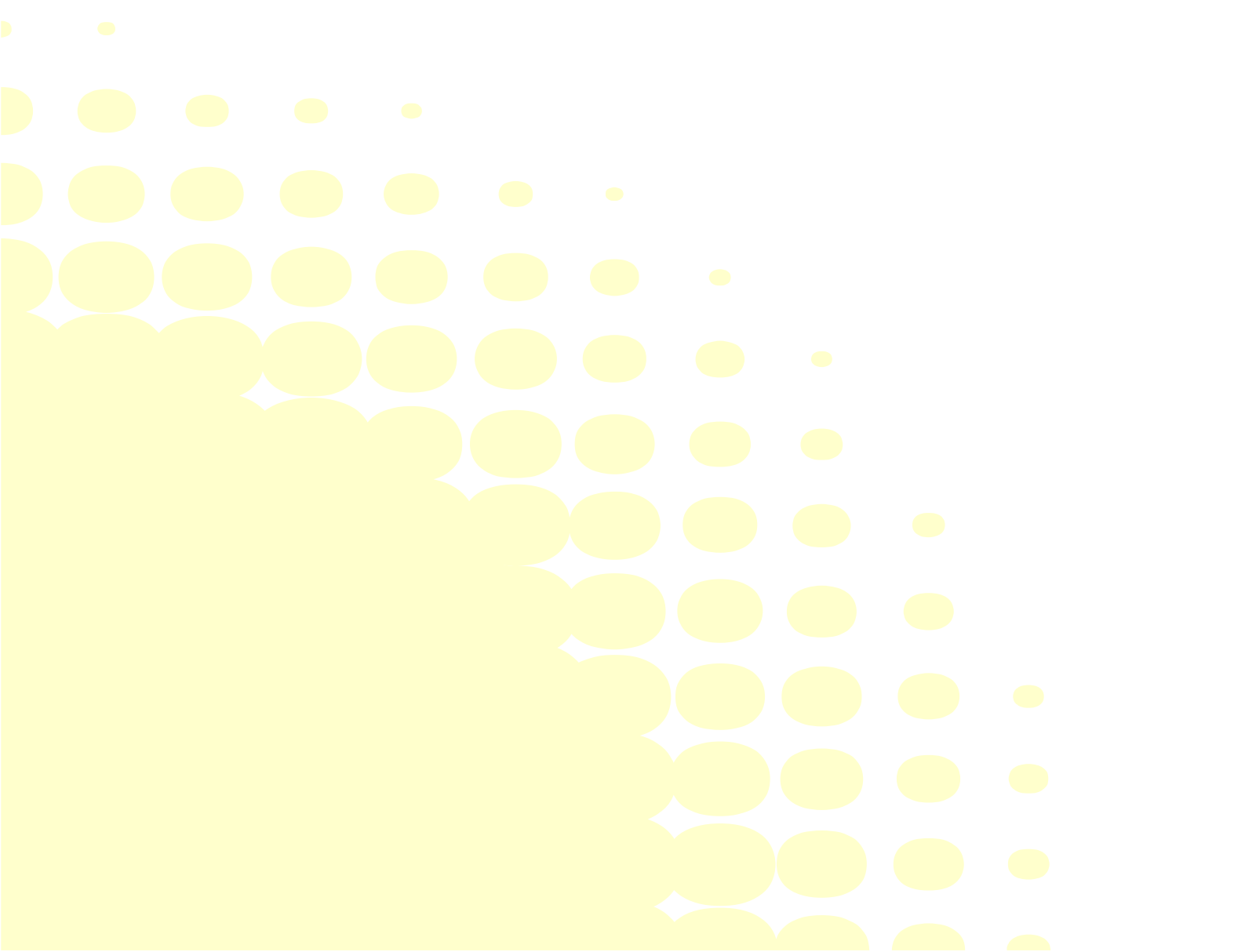
delivering



Confidentiality

e-Government Strategy Framework Policy and
Guidelines

Version 3.0
September 2002



Contents

1. Introduction	4
1.1 Ownership and maintenance of this document	4
1.2 Terminology	4
1.3 Who should read this document?	5
1.4 Background	5
1.5 Objective	5
1.6 Scope	5
1.7 Organisations affected by this document	6
1.8 Relationship to other framework documents	7
1.9 Availability of advice	8
2. Summary of government's approach to confidentiality	9
2.1 Introduction	9
2.2 Third party participation in provision of e-Government services	9
2.3 General approach to confidentiality	10
2.4 The PRIVATE descriptor	10
2.5 Information marking and handling	11
3. Confidentiality levels in government transactions	13
3.1 Introduction	13
3.2 Level 0 – transactions with no private information content	14
3.3 Level 1 – protection of minor private information	14
3.4 Level 2 – protection of sensitive private information	16

3.5	Level 3 – protection of very sensitive private information	17
4.	Risks and Countermeasures	21
4.1	Introduction	21
4.2	Stored data	21
4.3	Data being processed or in transit	22
A	Abbreviations	23

1. Introduction

1.1 Ownership and maintenance of this document

The e-Government confidentiality framework policy and guidelines document is one of a series developed as part of the Government's commitment, in the Modernising Government white paper¹, 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 policy² that sets out the e-Government security requirements. It specifically addresses those security requirements related to the provision of confidentiality services to support access to e-Government services.

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

1.2 Terminology

The following definitions are used in connection with the provision of e-Government services:

- a) **Confidentiality services.** These are the technical means by which assurance can be gained that private information is not accessed by or disclosed to those who are not authorised to receive it. These services include protection of stored data, and data being processed or in transit.
- b) **Private information.** Refers here to information relating to a specific client³ or government information⁴ involved in e-Government transactions for which there is a reasonable expectation that due care will be taken to keep it confidential.

The meaning ascribed to 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 *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 In the context of this document, a client denotes a person, an organisation, a representative of the person or organisation or a process.

⁴ Private information, in this context, might also include sensitive government information communicated in a transaction and ancillary information pertaining to e-Government services such as that detailed in sixth paragraph of section 1.6.

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

Confidentiality services protect private information from unauthorised observation and disclosure:

- a) when stored on e-Government systems.
- b) while in transit to, from, and within e-Government systems.

There are existing statutory requirements relating to the protection of personal data and communications under the Data Protection Act 1998⁵ and the Human Rights Act 1998⁶ as well as other legislative acts. This framework in no way dissolves the responsibilities of those implementing the guidance within it from adhering to all relevant aspects of UK law.

The privacy aspects of e-Government service provision are covered in the trust charter for electronic service delivery (e-trust charter)⁷.

1.5 Objective

This document is intended to set out a number of trust levels for confidentiality services in 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 document⁸.

1.6 Scope

This document is relevant to transactions and information handling involving private information.

⁵ Further guidance on the Data Protection Act can be found at <http://www.dataprotection.gov.uk>.

⁶ Further guidance on the Human Rights Act can be found at <http://www.humanrights.gov.uk>.

⁷ [http://www.e-envoy.gov.uk/oeo/oeo.nsf/sections/reports-top/\\$file/etrust_guide.doc](http://www.e-envoy.gov.uk/oeo/oeo.nsf/sections/reports-top/$file/etrust_guide.doc)

⁸ The latest version of *e-Government strategy framework policy and guidelines, security architecture*. Available at <http://www.e-envoy.gov.uk>

Information stored on a client's system is outside government control and is the responsibility of the client system owner.

This document addresses a category of electronic information not previously covered in government security guidance. It complements existing Cabinet Office guidance on safeguarding 'protectively marked' information (RESTRICTED, CONFIDENTIAL, *etc*) provided by the Manual of Protective Security (MPS).

It is anticipated that individual instances of private data handled by e-Government systems will not normally warrant a protective marking. However, there is a potential overlap between level 3 confidentiality and material given a RESTRICTED protective marking (see section 3.5.1).

In those cases where a protective marking is required, e-Government service providers and implementers can be provided with appropriate guidance from MPS. The case where this is most likely is in protecting major aggregations of private e-Government information. The detail of this is beyond the scope of this framework but, for indicative purposes, it is expected that such aggregations will normally warrant a RESTRICTED protective marking. Guidance from the MPS will always take precedence over that arising from the confidentiality framework.

This framework might also be applied to protection of ancillary information generated as a consequence of electronic service provision. System management information and information on the performance and uptake of e-Government services are examples. Information not covered by the MPS will be handled in line with this framework.

The physical and procedural security aspects are important elements of a multi-layer approach to the protection of private information but are not covered by this framework. Service providers will need to consider these aspects as part of the overall process for ensuring and maintaining confidentiality.

1.7 Organisations affected by this document

This framework applies to all electronic transactions carried out by or on behalf of government where there is a need for confidentiality. It is intended to ensure that all government bodies, and organisations providing service on their behalf, ensure confidentiality 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 confidentiality level;
- b) follow the guidance in this framework to deliver appropriate confidentiality processes and functionality for the assigned level;
- c) ensure that they have considered all of the risks set out in section 4 of this paper and applied the 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.

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 document⁹ 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 document¹⁰ 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 (this document) addresses the following objectives:

- a) OS8 – Privacy and confidentiality.

The business services framework document¹¹ addresses the following objectives:

- b) OS10 – Service availability;
- c) OS11 – Information availability;
- d) OS13 – Effective audit and accounting.

The network defence framework document¹² addresses the following objective:

⁹ The latest version of *e-Government strategy framework policy and guidelines, registration and authentication*. Available at <http://www.e-envoy.gov.uk>

¹⁰ The latest version of *e-Government strategy framework policy and guidelines, trust services*. Available at <http://www.e-envoy.gov.uk>.

¹¹ The latest version of *e-Government strategy framework policy and guidelines, business services*. Available at <http://www.e-envoy.gov.uk>

a) OS12 – Service protection.

The assurance framework¹³ 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 confidentiality framework may be obtained from the Office of the e-Envoy¹⁴.

CESG¹⁵ 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.

¹² The latest version of *e-Government strategy framework policy and guidelines, network defence*. Available at <http://www.e-envoy.gov.uk>

¹³ The latest version of *e-Government strategy framework policy and guidelines, assurance*. Available at <http://www.e-envoy.gov.uk>

¹⁴ <http://www.e-envoy.gov.uk>.

¹⁵ Telephone 01242 237323 or via <http://www.cesg.gov.uk>.

2. Summary of government's approach to confidentiality

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 confidentiality.

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 *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 provide confidentiality services to the same standards as government itself would. Government will in turn accept transaction data from those delivery channels, who will certify that they have carried out the transaction to the agreed standard.

2.2.2 *Use of commercial technologies*

Government will make use of normal commercial technologies and techniques for confidentiality services, subject to compatibility with these guidelines.

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 e-Government systems 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 confidentiality

For the purposes of e-Government transactions, this document defines levels of confidentiality that are appropriate for differing classes of transaction. In general, informal or lower value transactions will attract the lower levels of confidentiality services. Higher value or legally significant transactions will attract more stringent confidentiality requirements.

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

However, in practice, confidentiality is strongly linked to access control, and hence to the authentication process. If a transaction requires a high confidentiality level, it is likely to need an equivalent or higher authentication level.

If a real-world identity is required to engage in a transaction, it is likely that the registration level allocated will be equivalent to or higher than the confidentiality level, due to the role of registration in providing access control.

Confidentiality also depends upon both protection of the e-Government service provision domain as a whole against external attack, and the use of robust and reliable business service applications and infrastructure. These aspects are dealt with in the Network Defence and Business Services frameworks respectively.

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.

2.4 The PRIVATE descriptor

MPS has now introduced the concept of the PRIVATE descriptor. Moreover, the definition of RESTRICTED has been changed to remove a perceived implication that all information that falls under the provisions of the Data Protection Act (DPA) should be protectively marked RESTRICTED. By making this change it is recognised that the requirements of the DPA can be met through the application of the PRIVATE descriptor.

MPS states that: *'Within the UK there is no standard system for marking sensitive material that originates from outside central government. The sensitivity of these assets, particularly personnel information, is often indicated by the use of terms such as PRIVATE and CONFIDENTIAL or COMMERCIAL IN CONFIDENCE'.*

'Government Departments that manage or sponsor the management of e-Government services need to recognise the requirements of this security framework and supporting documents. Generally, information generated through e-Government services should carry the descriptor PRIVATE both to identify the type of data, but also to indicate that this security framework may apply.'

'Departments receiving PRIVATE data should value the data against the Protective Marking System and handle it accordingly. Even though a protective marking may not be appropriate, the data must be adequately protected. This can be achieved through the application of this security framework or at departmental discretion, by handling the data as RESTRICTED.'

'The PRIVATE descriptor may therefore be used either with or without a protective marking. Where a protective marking has been applied, departments should consider dropping the protective marking, but not the PRIVATE descriptor in further communications with the originator to avoid confusion or misunderstanding.'

2.5 Information marking and handling

It is suggested that information subject to the security framework should be marked as follows:

[PRIVATE], [Level n], [optional].

where PRIVATE is the PRIVATE descriptor, level refers to the confidentiality level as described in section 3 and optional is a descriptor tailored to the specific e-Government service. For example, medical information concerning an individual might be marked as PRIVATE, level 3, MEDICAL. The [] denotes an optional item.

It is envisaged that normally information that is assessed as requiring level 0 confidentiality will not attract the PRIVATE descriptor.

Information marked as PRIVATE should, at departmental discretion, be handled as RESTRICTED when in a government domain operating under MPS, but should not require baseline security measures when communicating with citizens or businesses that originated the information. Other government bodies (eg central government domains not operating under MPS and local authorities) will need to establish appropriate handling procedures.

3. Confidentiality levels in government transactions

3.1 Introduction

This section defines the four confidentiality levels, which represent degrees of impact of disclosure of private information. The levels are layered according to the severity of consequences that might arise.

It also gives examples of transactions and service provision guidelines (relating to service control objective OS8 – ‘Privacy and confidentiality’) under this scheme. Examples of transactions that might merit particular confidentiality levels are not intended to be definitive.

Service provision guidelines are divided into those that ensure confidentiality of stored data, and data being processed or in transit. Experience shows that electronic data is at its most prolonged exposure to potential risk whilst in storage. Effective protection of stored data is therefore considered to be the most important line of defence. Compliance with guidelines for record management systems, including document storage rules, will need to be considered as part of the specification of an e-Government service.

Nothing can be assumed about confidentiality in the client network domain. The service provision guidelines given here are thus mainly targeted at and applicable to government users.

In allocating transactions to confidentiality 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.

The impact of prosecution under the Data Protection Act and the consequent damage to reputation and other impacts (for example, the Information Commissioner has the power to order the cessation of processing of personal data) that might occur on breach of confidentiality must be explicitly considered in the allocation of the levels.

Departments must determine the level implied for each consequence and allocate the highest of these to the transaction. For example, if disclosure of transaction information might result in risk to the client’s personal safety, then the transaction must be allocated to confidentiality 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.

Aggregation of data at any level may require protection under a more stringent regime (*ie* may require to be treated as if it were assigned to the next level up). This might require protection in line with MPS at the higher levels.

Mobile devices (*eg* laptops) should only be used for the processing and/or storage of e-Government information if the extra physical security risks associated have been explicitly considered and reduced to an appropriate level. This might require more stringent security measures (such as routine encryption of contents and strong authentication of authorised government users) to be implemented than would be otherwise needed.

3.2 Level 0 – transactions with no private information content

3.2.1 Definition

Level 0 confidentiality is appropriate for e-Government transactions that involve **no private information content**. In particular, disclosure of transaction information at level 0 might result in at most:

minimal inconvenience to any party; or

no risk to any party's personal safety; or

minimal financial loss¹⁶ 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

An example of a transaction that might merit level 0 confidentiality is a client reading or downloading publicly available information from a government website. Disclosure of transaction information to a third party would cause no inconvenience or distress to any party.

3.2.3 Service provision

No explicit confidentiality protection is needed at level 0 though care should still be taken to adopt good system practice

3.3 Level 1 – protection of minor private information

3.3.1 Definition

Level 1 confidentiality is appropriate for e-Government transactions in which the information exchanged is client specific but where the impact of public exposure would be a **minor** resource or nuisance impact on one or more of the involved parties. In particular, disclosure of transaction information at level 1 might result in at most:

minor inconvenience to any party; or

no risk to any party's personal safety; or

¹⁶ In this context, 'financial loss' includes the results of any claim for damages.

minor financial loss to any party; or

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

minor distress being caused to any party; or

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 confidentiality include:

- a) a client e-mails a government department with a request for general information. Information involved in the transaction is client specific, but disclosure would result in minor inconvenience or embarrassment.
- b) receiving an e-mail indicating that more sensitive information is available for collection from a secure mailbox. Although the transaction is linked to more sensitive information, disclosure of this communication would cause at most minor impact.

3.3.3 Service provision

Confidentiality at level 1 requires attention to be paid to correct system operation and the use of basic access control¹⁷. At this level, it is generally acceptable to use the in-built security features of commercial products, configured correctly, but without enhancement.

Encryption of data is not necessary at level 1, whether the data is in storage or in transit, with the exception of certain niche areas (eg encryption of password files).

Private information displayed on a screen or printed out should be afforded an equivalent level of protection using physical and procedural security measures.

3.3.3.1 Stored data

Unpublished private information should be either stored on a system to which only authorised government users¹⁸ have physical access, or else should be password-protected¹⁹.

Unpublished private information accessible via open networks, such as the Internet, should be password-protected. Appropriate password management procedures should be devised and followed.

Systems storing unpublished private information should be subject to good system administration procedures.

3.3.3.2 Data being processed or in transit

Unpublished private information should only be processed on a system to which authorised government users have physical access or else should be password protected.

Systems processing unpublished private information should be subject to good system administration procedures.

¹⁷ Access control is discussed in *e-Government strategy framework policy and guidelines, security*. Available at <http://www.e-envoy.gov.uk>

¹⁸ A government user is defined as a person or process that interacts with an e-Government service from a back-office system or access service system (in any capacity). This includes third parties involved in the provision of e-Government services.

¹⁹ Password protection, where mandated, is a minimum requirement. Alternatives that provide greater protection without the use of passwords in particular are of course acceptable.

Information sent to clients should be sent to locations where there is a reasonable expectation of password-controlled access (eg. to an e-mail account operated by an Internet Service Provider). The onus will be on clients to nominate suitable locations, and on service providers to make clear to clients the impact on confidentiality should information be sent to locations for which access is not password controlled.

It is an acceptable risk at this level that e-mails will be correctly delivered as addressed.

3.4 Level 2 – protection of sensitive private information

3.4.1 Definition

Level 2 confidentiality is appropriate for e-Government transactions involving private information that could be regarded as sensitive. In particular, the impact of disclosure of transaction information at level 2 would be **significant** and might result in at most:

significant inconvenience to any party; or

no risk to any party's personal safety; 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

Examples of transactions that might merit level 2 confidentiality include:

- a) electronic filing of income tax and Value Added Tax (VAT) returns. Disclosure of transaction information in these cases might cause significant impact such as assistance in the commission of serious crime.
- b) financial transactions, in which the inadvertent disclosure of a debit card number, for example, would be likely to cause significant distress and inconvenience to a client.

3.4.3 Service provision

Confidentiality at level 2 requires auditable system operation and the use of stringent access control (see the second paragraph of section 3.4.3.1).

Use of cryptography to provide access control is appropriate for some purposes at this level.

At level 2 an independent IT health check should be considered for all systems hosting e-Government services.

Sensitive private information displayed on a screen or printed out should be afforded an equivalent level of protection using physical and procedural security measures.

3.4.3.1 Stored data

There is a strong requirement for protection of data via access control at this level.

Clients of e-Government services accessing sensitive private information are likely to be required to undergo authentication and registration²⁰ to at least level 2 in each case.

Government users who have access to bulk personal client information should be subject to at least as stringent requirements. The information accessible to system administrators should be the minimum necessary to meet the business needs.

Commercial operating system access controls should be employed for administrator access to systems.

Archived data should be stored such that only authorised and nominated individuals (in accordance with Data Protection law) have the right to access the data.

Strong access controls are required for access to bulk archive data. This may be achieved by physical or electronic access controls. Encryption of archives may permit the strong bulk data access control requirements to be reduced to a more tractable key management task.

Data stored in a live environment (eg. on a database) should be protected by strong access control. Encryption mechanisms present within the commercial operating system and database products may offer benefits but should be used only after their value has been established.

3.4.3.2 *Data being processed or in transit*

Sensitive private information should be processed on a system to which only authorised government users have physical access and should be password protected.

Processes handling sensitive private information should be tested to check for any inadvertent data leakage.

The required protection for data in transit at level 2 depends upon the nature of the communications path:

- a) for services provided over open networks, such as the Internet, some form of commercial encryption²¹ is appropriate. In the case of web-based services, HTTPS (HTTP over SSL) will usually be the most convenient protocol, owing to its inclusion in commercial web browsers. S/MIME v3 has been defined by the e-Government interoperability framework²² as the standard for secure email.
- b) for services delivered solely over the UK telephone network, there is no requirement for the use of encryption.

3.5 Level 3 – protection of very sensitive private information

3.5.1 *Definition*

Level 3 confidentiality is appropriate for e-Government transactions involving private information that could be regarded as very sensitive. The impact of disclosure of transaction information at level 3 would be **substantial** and might result in at most:

substantial inconvenience to any party; or

²⁰ Registration level is only relevant if a real-world identity is required to engage in the transaction.

²¹ Specific guidance on suitable technologies and products can be found in the lower level profiles and implementation documents.

²² <http://www.govtalk.gov.uk/interoperability/egif.asp>

risk to any party's personal safety²³; 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.

There is a potential overlap at this level with the RESTRICTED protective marking as set out in the MPS. The guidance in this section applies to information at level 3 confidentiality. If material is deemed to warrant a protective marking, the guidance from the MPS and related documents will always take precedence over that arising from the confidentiality framework.

3.5.2 Examples

Examples of transactions that might merit level 3 confidentiality include:

Electronic movement of a client's medical records. Disclosure of this information to an unauthorised third party might cause substantial distress and damage to the standing or reputation of the client.

3.5.3 Service provision

Confidentiality at level 3 requires auditable system operation and the use of stringent access control (see the second paragraph of section 3.5.3.1).

Use of cryptography to provide access control is anticipated at this level, based on use of a public / private key pair associated with a digital certificate.

At level 3 an independent IT health check is necessary for all systems hosting e-Government services.

Very sensitive private information displayed on a screen or printed out should be afforded an equivalent level of protection using physical and procedural security measures.

3.5.3.1 Stored data

There is a strong requirement for protection of data via access control at this level.

Clients of e-Government services accessing very sensitive private information are likely to be required to undergo authentication and registration²⁴ to level 3 in each case.

Providers and system administrators of e-Government services who have access to bulk personal client information should be subject to at least as stringent requirements. The information accessible to system administrators should be the minimum necessary to meet the business needs.

Consideration should be given to ensuring that all government users of systems processing or handling information at level 3 should be subject to a Basic Check security clearance.

Commercial operating system access controls should be employed for administrator access to systems.

²³ Note that the client may be a person, organisation, representative of the person or organisation or a process. Risk to the client's personal safety thus includes risk to the safety of installations as well as individuals.

²⁴ Registration level is only relevant if a real-world identity is required to engage in the transaction.

Archived data should be stored such that only authorised and nominated individuals (in accordance with Data Protection law) have the right to access the data.

Strong access controls are required for access to bulk archive data. This may be achieved by physical or electronic access controls. Encryption of archives may permit the strong bulk data access control requirements to be reduced to a more tractable key management task.

Data stored in a live environment (eg on a database) should be protected by strong access control. Encryption mechanisms present within the commercial operating system and database products may offer benefits but should be used only after their value has been established.

3.5.3.2 Data being processed or in transit

Very sensitive private information should only be processed on a system to which authorised government users have physical access and should be password protected.

Processes handling very sensitive private information should be tested to check for any inadvertent data leakage.

The required protection for data in transit at level 3 depends upon the nature of the communications path:

- a) for services provided over open networks, such as the Internet, some form of commercial encryption is appropriate. In the case of web-based services, HTTPS (HTTP over SSL) will usually be the most convenient protocol, owing to its inclusion in commercial web browsers. S/MIME v3 has been defined by the e-Government interoperability framework²⁵ as the standard for secure email.
- b) for services delivered solely over the UK telephone network, there is no requirement for the use of encryption.

²⁵ <http://www.govtalk.gov.uk/interoperability/egif.asp>

4. Risks and Countermeasures

4.1 Introduction

For all except anonymous services, the risks and countermeasures for confidentiality services include those identified for registration and authentication services, due to the role of access control in safeguarding confidentiality.

The *additional* risks applicable to confidentiality services follow below.

4.2 Stored data

Risk	Possible Countermeasures
R1) Access to computer system That unauthorised users may gain access to a computer system.	Possible countermeasures to ensure that unauthorised users do not gain access to computer systems include: C1) ensuring that users are authenticated before access to the system, down to the granularity of a particular user (for both clients and government users).
R2) Access to data That authorised users may access data they are not authorised to see.	Possible countermeasures to ensure that authorised users do not gain access to data they are not authorised to see include: C2a) using the operating environment access control mechanisms for which authenticated clients and government users are only allowed to access the data for which they have the corresponding rights. Superuser accounts will be avoided as far as practicable; C2b) employing encryption as an access control mechanism for stored data. If data is encrypted, then an equivalent access control regime must be applied to the encryption keys.
R3) Access to web services That unauthorised users may gain access to limited-access web services.	Possible countermeasures to ensure that unauthorised users do not gain access to limited access web services include: C3a) authentication of users before access to the web server, down to the granularity of a particular individual or process; C3b) allowing authenticated users access to only those web services for which they have the corresponding rights.

4.3 Data being processed or in transit

Risk	Possible Countermeasures
<p>R4) Inadvertent disclosure</p> <p>That data may be inadvertently disclosed during processing. Disclosure might be by erroneous display on a screen, inclusion in a print out or being attached to data being legitimately and correctly sent to a third party.</p>	<p>Possible countermeasures to ensure that there is no inadvertent disclosure during processing include:</p> <p>C4a) authentication of government users prior to accessing the system or process;</p> <p>C4b) use of structured design techniques;</p> <p>C4c) appropriate and careful testing of the application;</p> <p>C4d) marking (eg by use of a digital signature) all data that is to be correctly released and testing for this as part of any display, print or export process.</p>
<p>R5) Misdirection</p> <p>That an electronic communication may be misdirected accidentally or intentionally to an individual or process not authorised to see it.</p>	<p>Possible countermeasures to ensure that communications are not misdirected include:</p> <p>C5) confining communications to trusted channels or networks.</p>
<p>R6) Interception</p> <p>That an electronic communication may be read by unauthorised individuals or processes as a consequence of interception or misdirection.</p>	<p>Possible countermeasures to ensure that communications are not intercepted include:</p> <p>C6a) ensuring that the communication channel is adequately protected against interception (eg physically);</p> <p>C6b) if the risk to the communication channel warrants it, the encryption of the communication contents (eg using S/MIME or HTTPS (HTTP over SSL));</p> <p>C6c) encryption of the communication contents with the public key of the correct recipient.</p> <p>Additionally:</p> <p>C6d) persons found to be intercepting communications in breach of UK law may be prosecuted.</p>

A Abbreviations

DPA	Data Protection Act
MPS	Manual of Protective Security
PC	Personal Computer
PKI	Public Key Infrastructure
VAT	Value Added Tax

© Crown Copyright 2002

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

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

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

