Office of the *e-Envoy*

Leading the drive to get the UK online

delivering

UK online

Security

e-Government Strategy Framework Policy and Guidelines

Version 4.0
September 2002

Preface

By Andrew Pinder, e-Envoy

Government has committed to deliver its services in ways that meet the desires of the citizens and businesses it serves, enabling them to interact securely in places and at times that are convenient to them. We recognise that engendering trust and confidence is vital to increase the uptake of e-government services. This e-Government Security Framework provides key guidance to service providers wishing to gain the trust and confidence of their users. It lays the foundations for enabling secure services to be provided that will truly transform the way we interact with government.

This framework is aimed at those establishing, procuring and providing e-Government services. Chief Executives and Senior Responsible Officers should ensure that their business risks are appropriately addressed in accord with this guidance.

This over-arching document is supported by other documents in this framework, covering Assurance, Business Services, Confidentiality, Network Defence, Registration & Authentication and Trust Services. They embody the internationally recognised information security standard, BS EN ISO 17799, with which all key government information processes should shortly be compliant. The risk assessment approach promoted by this standard encourages appropriate security measures to be applied. This is further augmented, in these documents, by inclusion of best practice from both the private and public sectors, providing guidance that is truly useful at the practical level.

We will review the documents as practice evolves. In addition we intend to publish detailed lower level guidance to supplement and strengthen the message.

Contents

1. Introduction and scope

1.1 Introduction

The e-Government security framework is one of a series developed as part of the Government's commitment, in the Modernising Government white paper[1], to producing 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.

1.2 Terminology

The meaning ascribed to specific terms within this security framework document and the related lower level documents is provided in the glossary at annex A[2]. A list of abbreviations specific to this document is provided at annex B.

1.3 Who should read this document set?

This document and its related lower level documents (see the document model at section 1.7) is aimed at those establishing, 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

It is the aim of the Modernising Government programme to move towards the electronic delivery of government services. To this end, Government has produced an e-Government strategy.

---

[1] *Modernising Government white paper.*

[2] This glossary also supports the various lower level security framework documents.

1.5   Objective

This document sets out a framework for the expression of security requirements for the procurement and acceptance of e-Government services and their implementation. It also describes the approach to assuring the presence and proper operation of the security countermeasures put in place to meet the security requirements.

This framework document and others derived from it are intended to be implementation independent expressions of security requirements. Implementation constraints are limited to only those necessary to meet government security requirements. Suppliers are free to propose differing implementations constrained only by any interoperability requirements that may be necessary for operational reasons.

This framework document does not identify specific services as it is intended to apply to the provision of services in general. Annex C presents a set of example scenarios that illustrate many of the security issues to be addressed. This list is not intended to be complete and will be added to and amended as experience with electronic service provision develops.

The security requirements expressed in this framework document represent a call for general alignment with best e-commerce practice, to which government believes it must itself conform.

This document currently addresses only functional security requirements and those non-functional aspects of the implementation that permit the services to be readily assured. Assurance will also be needed to ensure the presence and proper operation of those functions. This is discussed further in section 1.7.

1.6   Scope

The scope of the security framework is summarised below and discussed further in section 2.

The scope includes functional security requirements appropriate for the delivery of e-Government services by, and on behalf of, government. It is applicable to all systems responsible for the delivery of e-Government services to citizens, businesses and other organisations, including:

a)   access services and systems; an example of an access system is the current Government Gateway;

b)   back-office services and systems that work in conjunction with the access services and systems to provide a particular end-to-end e-Government service.

The security framework does not explicitly cover government to government transactions unless this is part of an e-Government service with a citizen or organisation.

Some systems (*eg* a back-office system within a department) may be subject to other security requirements (*eg* the Manual of Protective Security (MPS)). In the event that there is a conflict between the security requirements set out in the security framework documents and other applicable security requirements, the order of precedence is:

a)   MPS, where it applies;

b)   the security framework documents;

c)   other security documents.

There is a stated intention to converge MPS and the e-Government security frameworks in the future.

It is not the intention that the security requirements set out in the security framework documents should be applied retrospectively to existing systems. However, it is envisaged that these should be addressed for modifications to existing systems that are relevant to the delivery of e-Government services.

The security requirements set out in this framework are also applicable to the delivery of government services by third party organisations.

1.7   Document model for e-Government security requirements definition

The framework document is a high-level expression of security requirements and expands upon the security statements in the e-Government strategy ["e-citizen e-business e-Government"]. It also sets out the process for determining the security requirements and assuring the presence and proper operation of the security countermeasures put in place to meet the security requirements. Other related and more detailed security requirements and process statements address specific topic areas. Figure 1-1 below depicts the relationships.
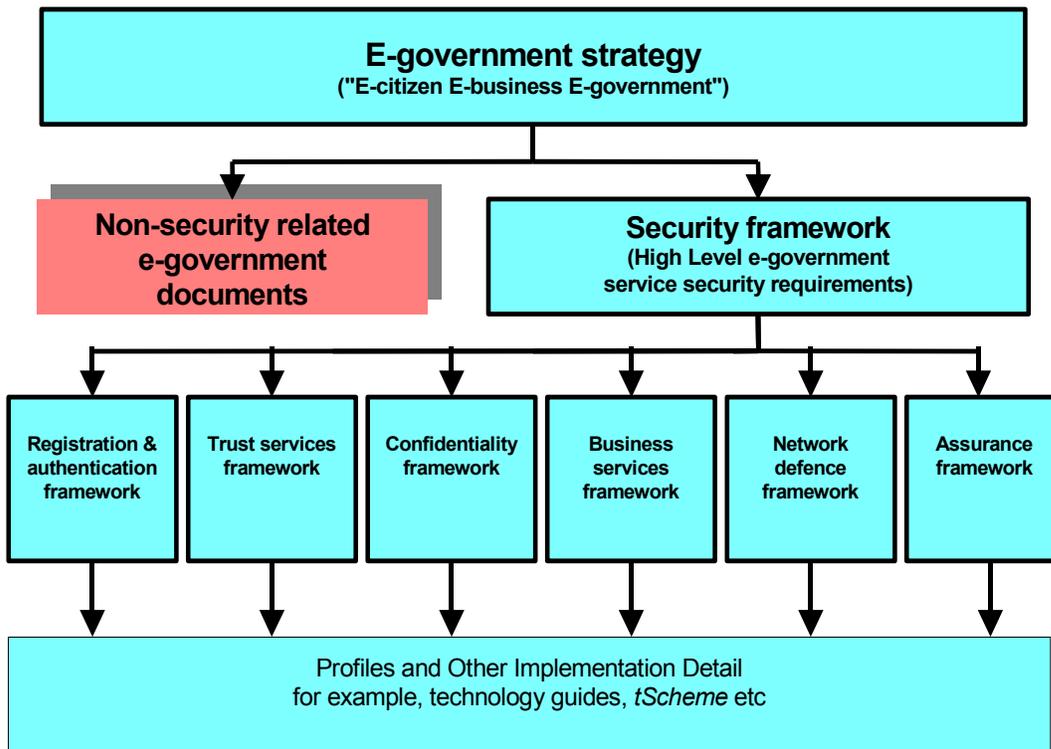
Figure 1-1: Security framework documents

This high level security framework is supported by more detailed framework statements for the specific topic areas below:

a. The **registration and authentication framework**[3] covers the security services required to ensure that all users[4] are uniquely and unambiguously identified[5] and granted access only within the authorisations made. All systems security ultimately rests upon the capability to identify and appropriately authenticate and enforce clients and all other users' privileges in respect of the system assets.

b. The **trust services framework**[6] covers the security services required to ensure that transactions are properly traceable and accountable to authenticated clients or other users and cannot subsequently be disavowed.

c. The **confidentiality framework**[7] covers the security services required to ensure that information is stored securely and not disclosed to persons or processes unauthorised to see it.

d. The **business services framework**[8] covers the security services required to ensure that the e-Government service applications themselves are designed, developed, configured and operated in a secure and robust manner and their information assets properly protected. This includes disaster recovery and business continuity.

e. The **network defence framework**[9] covers the security services required to ensure that the plant, stored data and other assets of the e-Government service are properly protected against malicious or inadvertent electronic attack.

f. The **assurance framework**[10] addresses the means by which trust in the implementation of security elements can be assured.

There are also a number of relevant lower level documents that will be published from time-to-time. These include the e-Government interoperability framework (eGIF). These lower level documents will provide, for example, detailed implementation guidance.

While the security framework and related documents are implementation independent, an illustrative security architecture has also been produced[11] within the context of the current government gateway

---

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

4 A user is a person or process that interacts with an e-Government system (in any capacity). A client is a person, an organisation, a duly authorised representative of the person or organisation or a process seeking to carry out a transaction with government. Users include clients and all other staff who manage, operate or administer the e-Government service electronically.

5 Throughout this framework, a distinction will be made between an *electronic identity,* which is used to denote a set of information that uniquely identifies a client to a computer system (such as username or digital certificate) and a *real-world identity.* The electronic identity will necessarily belong to a real-world identity (a person, an organisation, a representative of the person or organisation or a process), but this real-world identity need only be revealed if it is necessary for the transaction. The word 'identify' is used here to denote an association with an electronic identity as a minimum.

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

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

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

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

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

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

approach. In particular, it provides particular illustrative on-line business scenarios at various levels of trust with currently available technologies and processes.

1.8   Overall approach

The approach for security requirements expression used throughout the security framework documents is based upon the Protection Profile concept developed for the international security evaluation criteria (Common Criteria). This concept is summarised at annex D. The security requirements are presented in terms of the following:

a) The security environment (see section 4) is a statement of the security problem by identifying the assets, which are to be protected, the threat agents who might represent a threat to those assets, and the specific threats to those assets. A threat is a particular attack that exploits an asset vulnerability.

b) The security objectives (see section 5) are a concise statement of a set of control objectives which, when achieved, will result in the required protection being achieved.

c) The security requirements (see section 6) are a set of technical security requirements statements against which any implementation can be tested.

The more detailed lower-level framework documents (see section 1.7 and section 5.4) describe the various levels of security requirements.

1.9   Use of Public Key infrastructure

In the lower level documents many of the security measures that can be put in place to meet the security requirements assume that a viable and coherent Public Key Infrastructure (PKI) based on digital certificates will be increasingly available. Pragmatic, but less inherently secure, measures are also offered in the near term, where appropriate. The use of such alternatives needs to be discussed and agreed as part of the development and agreement of the security concept (see section 3.2 Service concept development) for a specific e-Government service.

1.10 Availability of advice

In the first instance, advice on the application of the security 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.

---

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

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

2. Service security environment

2.1   Environment assumptions

To meet the objectives of e-Government, it is assumed that the delivery of government services will share the same public network infrastructure that is being used in the community at large. In particular, the Internet will be a principal means by which public access to government and government services will be achieved though others such as interactive digital television and call centres will be used.

2.2   Domain model

A typical e-Government service will involve a number of different management regimes referred to as security domains. Different security assumptions apply to each domain. For example, one security domain might be entirely under the control of the client, while another might be completely under the control of the service provider. The security domain model is illustrated in Figure 2-1 below.
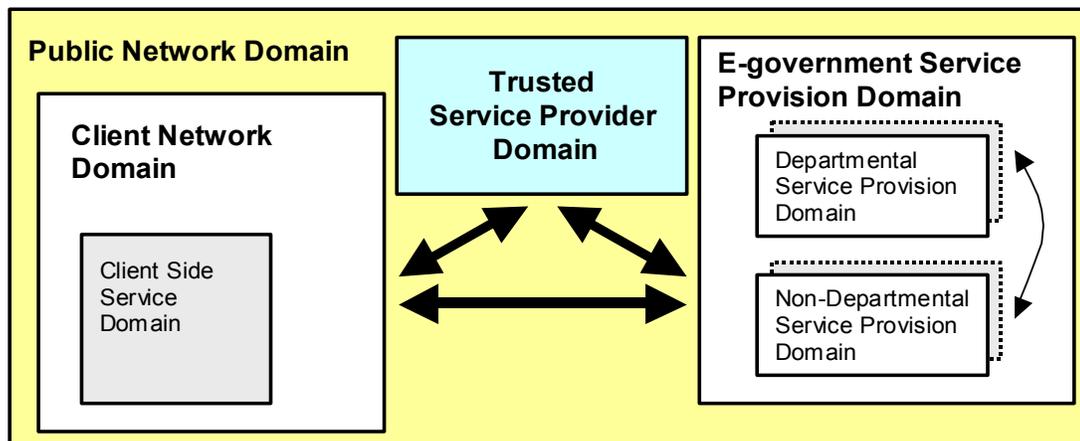
Figure 2-1: Security domains

The **Public Network Domain (PND)** contains that part of the communications infrastructure that lies outside the control of clients or e-Government service providers or government users or their representatives (eg third party providers). In the case of Internet delivery, it must be assumed to be accessible to potential threat agents and provide a transmission capability with no service quality commitments. In the e-Government context, the PND includes the Internet and service providers that

provide the Internet access and may also include the PSTN, interactive TV and other communications platforms.

The **e-Government Service Provision Domain (ESPD)** contains the access systems that are under service providers' control and used to host e-Government services. In the current e-Government architecture the ESPD is essentially viewed as including both the government gateway and the Government Secure Internet (GSI) together with other private networks (eg the private networks for Local Authorities). Where services are jointly provided by different, possibly non-government, organisations, the ESPD security requirements will apply across the heterogeneous network infrastructure supporting the services. It is a requirement that the ESPD be adequately protected against outside attack in accordance with applicable policy.

A **Departmental Service Provision Domain (DSPD)** contains IT infrastructure used to host all or part of a government service and is under the management control of the department offering the service. The DPSD is assumed to lie wholly within the ESPD that is used to communicate between different DPSD regions. For this reason it is preferable that all e-Government departments subscribe to, and use, the GSI for direct provision of e-Government services.

A **Non-Departmental Service Provision Domain (NDSPD)** contains IT infrastructure used to host all or part of an e-Government service supported by a non-departmental body and is under the management control of the organisation offering or contributing to an e-Government service. The NDSPD is assumed to lie wholly within the ESPD that is used to communicate between the distributed service elements. It is preferable that a NDSPD be accommodated within the GSI or other secure networks within the ESPD. If this is not the case, service providers will have to demonstrate that the security requirements have been satisfied external to the GSI.

A **Client Network Domain (CND)** is that element of the IT infrastructure under management control of the client, which is used to support access to the government services. The CND may be a single domestic Personal Computer (PC) connected via an ISP to the ESPD, in this case the ISP lies within the PND. Alternatively, the CND may be a complete corporate Intranet comprising many workstations under a more formal control. The practical level of trust in the CND will depend on the extent of the management controls exercised but, as it lies outside the ESPD, no assumptions of trust can be made about the CND environment. The CND includes the client in that he/she has a responsibility for protecting his/her own information.

The **Client Side Service Domain (CSSD)** is that element of the CND that is supplied by or on behalf of e-Government services and installed within the CND to encapsulate important trusted elements. e-Government service management will exercise some control over the content of (but not necessarily the delivery of) the CSSD. The goal is to deliver the CSSD functions embedded in a trusted Smart Card or similar token though initial deployments may not achieve or require this. The CSSD may, subject to appropriate security controls, be updated periodically by use of downloaded or distributed software. The client has a responsibility to ensure that such trusted elements are protected appropriately.

The **Trusted Service Provider Domain (TSPD)** is that element of the e-Government service infrastructure that is operated under a service agreement on behalf of government by a commercial service provider. The TSPD is operating as an agent of government and is expected to meet the standards necessary to act as a government agent or proxy. In general, security requirements levied

on the ESPD are applicable to the TSPD and will form part of the conditions of operation. The TSPD will typically be connected only to the PND but will have a privileged relationship with the e-Government service providers.
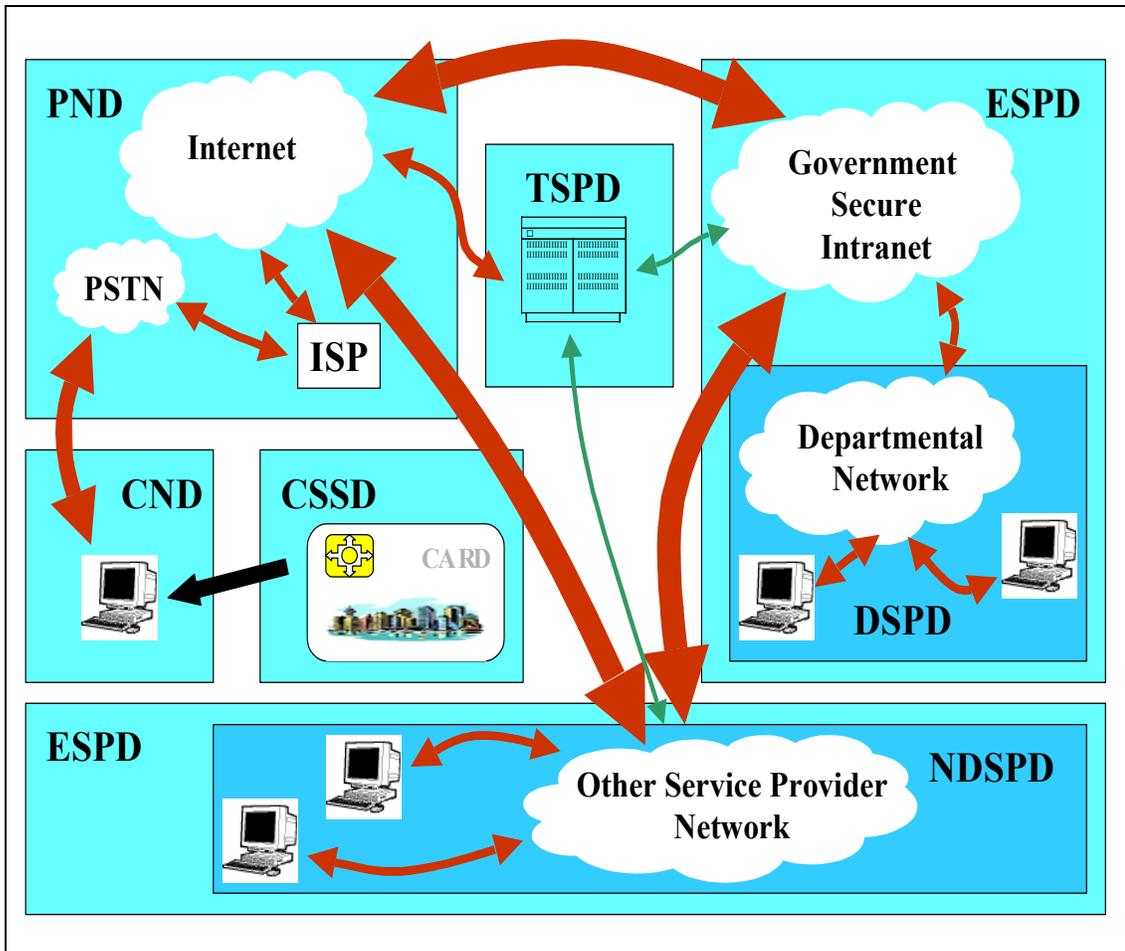
Figure 2-2: Example e-Government service delivery model

Figure 2-2 above illustrates how these security domains map on to one envisaged implementation approach for government service delivery via the GSI and Internet to a client's domestic PC.

2.3   External security policy framework

The implementation of e-Government services must take place within the legislation that applies to the handling of national/international, commercial, and personal information within public and corporate networks and information servers.

The individual Departments, non-departmental public sector bodies, Local Authorities and other local government bodies will also possess their own corporate information handling and security policies, which provide more detailed interpretations of the national or corporate policy and legislative frameworks and address the business continuity requirements of the organisation. Organisational policies are not cited explicitly but are assumed to express requirements for good business practice. In addition, government aims to take a lead in the setting of and conforming to high standards of management in its control of publicly owned assets and information.

The principal pieces of legislation that inform the security requirements for e-Government implementations include and are not limited to:

a) The **Human Rights Act** and the underlying European Convention on Human Rights set out everyone's right to privacy in their correspondence.

b) The **Data Protection Act (DPA)** sets requirements for the proper handling and protection of personal information held within information processing systems.

c) The **Electronic Communications Act** sets the requirements for electronic signatures and their equivalence to conventional signatures.

d) The **Regulation of Investigatory Powers Act** makes it an offence to intercept communications on any public or private network. Case and time limited exemptions may be granted subject to warrant.

e) The **Terrorism Act** makes it an offence to take actions which are designed seriously to interfere with or seriously to disrupt an electronic system.

f) The **Wireless Telegraphy Act** controls the monitoring of wireless telegraphy.

g) The **Police and Criminal Evidence Act** defines conditions under which law enforcement may obtain and use evidence.

h) The **Computer Misuse Act** makes attempted or actual penetration or subversion of computer systems a criminal act.

i) The **Public Records Act** lays down requirements for the proper care and preservation of documentary records of government activities.

j) The **Official Secrets Act** lays down requirements for the proper control of government information.

k) The **Freedom of Information Act** lays down the citizen's rights of access to government held information.

2.4   Extant security standards

BS7799[14] presents a code of practice (Part 1) and requirements specifications (Part 2) for establishing, implementing and documenting the security of information management systems. It provides a set of controls which, when implemented, will ensure best practices for e-Government services in specific installations are met.

It is government policy to move to BS7799 compliance. If required, certification to BS7799 can be achieved by any accredited BS7799 certification agency or by a suitably qualified internal auditor.

Part of BS7799 compliance is a full risk assessment. The government-preferred method is a CRAMM review and an HMG Infosec Standard 1 analysis. The approach to risk assessment should be agreed with the accreditor as part of the security concept phase (see section 3.2 Service concept development).

The Manual of Protective Security contains general security requirements and guidance for the handling of protectively marked information, in both electronic and other forms. It is the reference document for information marked RESTRICTED and above and should be used when interpreting the framework security requirements for protectively marked information. It provides the government guidance for the implementation of BS7799 controls for protectively marked material.

ITSEC and the Common Criteria for IT Security Evaluation provide a set of functional classes and assurance criteria upon which a formal evaluation and certification process can be based. The extent to which formal evaluation is applicable to e-Government services has yet to be established.

tScheme is the co-regulation scheme for Trust Service Providers in the UK and has developed a set of registration profiles and an assessment scheme to demonstrate profile conformance. e-Government services will make use of external Trust Service Provision and may therefore wish to call up the *tScheme* profiles as part of an e-Government trust service provision agreement. Government has published its own minimum requirements for verification of the identity of individuals[15] and organisations[16].

---

[14]   BS7799-1:1999 and BS7799-2:2002. BS7799 is also an International Standard (ISO 17799).

[15]   *e-Government strategy framework policy and guidelines HMG's minimum requirements for the verification of the identity of individuals (under revision following public consultation).*

[16]   *e-Government strategy framework policy and guidelines HMG's minimum requirements for the verification of the identity of organisations (under revision following public consultation).*

3. How to use the security framework

3.1 Introduction

The security framework documents represent a baseline and guidance for discussions and agreements as to what constitute adequate and acceptable security measures for the implementation of a particular service during each phase of the development and introduction of a new or enhanced e-Government service. This section sets out the process for determining the security requirements and assuring the presence and proper operation of security countermeasures meeting the security requirements.

3.2 e-Government security process

It is envisaged that the introduction of a new or enhanced e-Government service by a central or local government organisation will go through the following generic phases, illustrated in Figure 3-1 below. This model represents both one-off projects for implementing a system, which can be fully defined in advance, and more incremental or evolutionary developments where new service requirements are added later.

Consideration of how the information held and processed by the e-Government service is protected is an essential element of each of these phases and is an integral part of the definition, implementation and delivery of an e-Government service. The approach is outlined in the following paragraphs.

The term business sponsor is used to refer to the individual within the government organisation with overall responsibility for the provision and security of an e-Government service.

Service delivery is by one or more service providers each of which could be a government organisation or a third party. For example, service might involve a number of government organisations, each of which contributed to the overall e-Government service. A government organisation might provide that element by itself or might use a contractor.

Security activities would be split between the business sponsor and the service provider, depending on the commercial arrangements. It is assumed, however, that the security accreditor would be independent of the service provider.
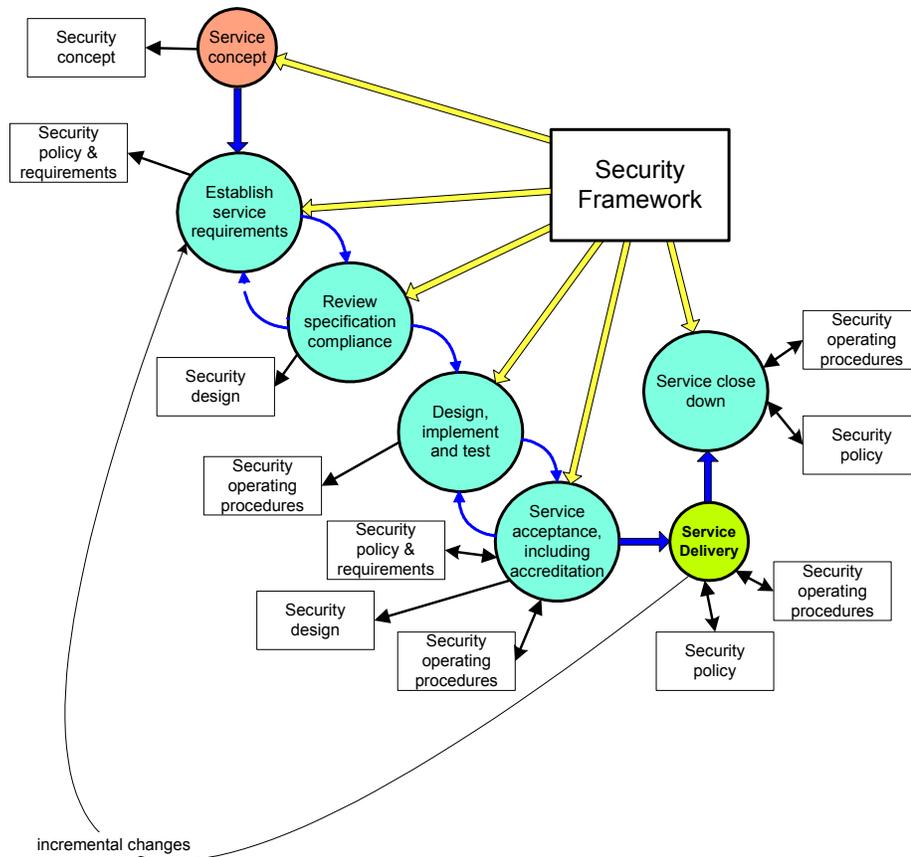
Figure 3-1: Application of framework

Service concept development

A key output of this phase is a documented security concept for the business service, including:

a) the key elements of the planned e-Government service and how it is planned to deliver the service (*eg* identification of each government organisation or third party responsible for delivering an element of the e-Government service);

b) an initial identification of the security domains and the applicable security regime for each particular security domain (*eg* the security framework might be applicable to the client side and access services and MPS might be relevant to the back-office systems); this also includes the need to establish the mechanisms for accreditation across domain boundaries;

c) an initial threat assessment, including a review of the information and service delivery assets that need to be protected and the likely threats;

d) an initial assessment (see below in Service requirements specification and review of compliance) of the security requirements to be met by the proposed service, based on an initial threat and risk assessment; for example, in domains where the security framework applies;

e) an initial assessment of the need for security operating procedures and handling instructions for the information handled by the specific e-Government service;

f) an assessment of whether the service concept is feasible from the security perspective; security considerations may possibly lead to changes in the service concept;

g) consideration of how well the service will work with other business services operated by or on behalf of government, both in terms of presentation and functionality.

It is envisaged that the appropriate accreditor is identified early in this phase. The accreditor provides advice to the business sponsor on all security aspects.

Service requirements specification and review of compliance
Specification and review of the detailed security requirements is undertaken in parallel with the development and review of the service specification. The accreditor provides advice to the business sponsor on all security aspects and reviews all security-relevant documentation.

This phase includes a detailed review of the information and service delivery assets, and an analysis of the threats and vulnerabilities, leading to a risk assessment. The security requirements to be met by the e-Government service are then set in response to the risk assessment.

The lower level security framework documents provide a standard approach to the risk assessment. Levels of risk are determined by assessing the impact of the following threat factors:

a) misappropriation of real-world identity;

b) misappropriation of electronic identity or access credentials;

c) failure to keep commitments made;

d) disclosure of private information;

e) non-malicious failure of the service and/or infrastructure;

f) a malicious or inadvertent electronic attack.

The severity of the impact: is assessed by examining the consequences of a number of different impact types as shown in Table 3-1. The severity is categorised from minimal (level 0) to substantial (level 3) for each impact type with the greatest impact setting the level.

Impact type	Level 0	Level 1	Level 2	Level 3
Inconvenience	Minimal	Minor	Significant	Substantial
Financial loss	Minimal	Minor	Significant	Substantial
Damage to standing or reputation	None	Minor	Significant	Substantial
Distress	None	Minor	Significant	Substantial
Release of personally or commercially sensitive data to third parties	None	None	Some	Some
Assistance in the commission of or hindrance to the detection of serious crime	None	None	Some	Some
Risk to personal safety	None	None	None	Some

Table 3-1: Summary definition of security levels

Part of this risk assessment covers the establishment of a coherent set of levels, as assessments in one area might lead to a constraint in another area. For example, it might be necessary to have a higher level for misappropriation of identity to support the delivery of particular commitments than might otherwise be necessary. The overall set of levels is referred to as a levels profile. The required profile is the minimum levels that meet all the assessments and related constraints.

The lower level security framework documents also provide standard security countermeasures appropriate for each level of risk.

The assessment should also cover establishing the appropriate physical, procedural and personnel[17] security requirements applicable to the system. These in conjunction with the electronic security requirements set out in this security framework provide a layered defence against the various threats.

It is envisaged that the functional and non-functional security requirements would be documented as part of the security policy (preferably compliant with BS7799) that would be produced during this phase.

Part of the service specification and review stage will include establishing the service specific policies for retention and secure storage of information processed or stored by the service. Some information may need to be maintained for long periods (eg medical records).

The security environment and related physical, procedural and personnel security measures for the service design, development and test phase also need to be identified and agreed during this stage.

Service design, implementation and test
Design, implementation and test of the security aspects of the e-Government service are undertaken in parallel with the service design, implementation and test activities. The security design proceeds by:

a) addressing the risks with appropriately assurable countermeasures;

b) locking-down the architecture to cover only required services;

---

[17] The physical, procedural and personnel security requirements are outside the scope of this security framework document. Guidance is provided by the Manual of Protective Security or BS7799, as appropriate.

c) assessing the residual risk and repeating steps a) and b) until the residual risk is acceptable.

The accreditor provides advice to the business sponsor on all security aspects and reviews all security-relevant documentation, including, for example, a security design, describing how the various security objectives will be met, or security-relevant test results.

This stage includes an assessment of whether the controls available from off-the-shelf software are satisfactory or whether the controls should be augmented by bespoke software elements.

The system design could involve development of a bespoke product from scratch or the identification and possible modification of a suitable existing or off-the-shelf product. In either case, care should be taken in the design process to meet all the previously identified functional and security requirements. Modularity of design is generally regarded as best practice, not least because it makes risk management much simpler.

If generic products are used, it must be ensured that they are fit for purpose and identified how they might need modifying or configuring for government use.

Service implementation includes:

a) development and/or configuration of the security countermeasures;

b) establishment of the security relevant processes for the operation and management of the e-Government service, including audit and accounting;

c) the development and approval of security-relevant documentation, including a security design and detailed security operating procedures for the access system and back-office elements responsible for service delivery;

d) the development and approval, where necessary, of handling instructions for the information associated with the specific e-Government service, covering, for example, disposal of printed material, media, transmission rules etc;

e) development of security statements and advice for clients of the business service. The following should be considered:

- a privacy statement for the business service, covering the information provided by the client, including what uses it would be put to and to whom it might be distributed;

- acceptable client hardware and software for the secure use of the e-Government service;

- the necessary information that a client should supply for enrolment for specific transactions;

- retention periods for information supplied to or by the business sponsor;

- an overview of the security protection in place;

- security advice to clients (eg password/PIN change times).

Service testing includes:

a) checking that the system configuration is compliant with security policy;

b) testing that the security countermeasures are implemented according to the design;

c) testing that the various security processes work and are documented correctly;

d) carrying out any additional security tests required for demonstrating the required assurance.

Service acceptance, including security accreditation
Security accreditation is undertaken in parallel with the acceptance procedure for the service. The business sponsor, based on the advice from the accreditor, and taking into account the trade-offs between residual risk, the benefits of the e-Government service and security relevant test results, is responsible for accrediting the operation of the service.

Service delivery
During the operation of the service, the e-Government service provider is responsible for day-to-day operational security in line with the security operating procedures.

During the operation of the service, the business sponsor is responsible for:

a. ensuring that regular software maintenance is carried out to ensure reliability and availability of service;

b. periodically reviewing the assurance and the effectiveness of the security countermeasures in conjunction with the accreditor;

c. initiating corrective action in response to identified security weaknesses or changed threats or circumstances;

d. ensuring that security is taken into account when any incremental changes to the e-Government service are planned.

Service close down
Once the service is no longer required, the business sponsor is responsible for ensuring that information assets are removed and transferred to a successor service, if appropriate, destroyed or stored securely in accordance with the service specific policies.

3.3   Use of security framework documents

The security framework documents provide a set of threats, security objectives and security requirements that are applicable to the delivery of e-Government services.

During the e-Government security process set out above, it is recognised that, subject to a risk assessment, not all security requirements may be applicable in all cases, and that in some cases it may be technically or economically infeasible to meet the requirements fully. Such issues should be documented as part of the security concept and / or the security policy and agreed using the review process set out above.

When using these requirements as a basis for assessing the acceptability of a potential service offering, the aim should be to meet those security requirements that are applicable to the specific service. Where a security requirement is not met, the reasons for this must be documented and agreed with the relevant accreditor as acceptable.

4. Threats to e-Government services and clients

In considering the protective measures that should be put in place within e-Government systems, a risk analysis must be performed. This risk analysis must consider the intent, motivation and capability of sources of threat, the feasibility and potential frequency of methods of attack, the nature of vulnerabilities that may be exploited, the value of assets to be protected, the consequences of a successful attack, and the costs of any countermeasures.

Threat analysis examines the assets that require protection, the potential sources of threat and the likely methods of attack. Annex E describes some threat scenarios that are relevant to e-Government services and clients.

4.1   e-Government service assets

The following are assets of e-Government based services which require protection:

a)   The personal data relating to a client for any e-Government service must be protected against loss, damage, or unwarranted disclosure in line with the relevant data protection and privacy legislation. It is important to note that personal data, once transferred to the CND from the e-Government service, is outside the scope of the e-Government service, which can take no responsibility for it. All clients are responsible themselves for the proper protection of their personal details when they are under their personal control.

b)   The corporate information base of government in general and organisations offering e-Government services must be protected against loss, unwarranted disclosure or introduction of erroneous content.

c)   The e-Government service (comprising the applications and delivery platforms) must be protected against threats to its availability and the integrity of the service offered.

d)   Authentication credentials must be protected against forgery or unwarranted use.

e)   Objects that represent monetary or other value must be protected against fraud. Some of the e-Government transactions are likely to result in cashable orders, which must be properly controlled, some may relate to the delivery of goods that can be misappropriated.

4.2 Potential sources of threat

An authoritative statement on the level of threat that potential threat agents pose will be required on a regular basis in order to ensure that adequate countermeasures are in place[18].

A particular threat agent may have consequences for either the e-Government service provider or for the client. For example, inadvertently or maliciously providing incorrect travel information to a client could lead to significant inconvenience.

4.2.1 Internal sources of threat

Some of the potential threat agents are clients, e-Government service operators and insiders for whom system authorities have some responsibilities and can exercise some control. These include:

a) **Legitimate clients** of e-Government services may seek to misuse or damage e-Government service provision. Such individuals may possess, or have access to, significant technical resources and skills with a strong motivation to subvert the service – frequently for financial gain. Hostile clients will have full access to their own CND from which to attack the service. Legitimate clients of the service are likely to be subject to legal restraint if subversive activity is traced to them. Legitimate clients of e-Government services may also unintentionally damage e-Government services. This is most likely to arise as a result of genuine mistake or non-intuitive service design. Such individuals are not generally motivated to undermine the e-Government service provision but may nevertheless cause significant disruption. A legitimate client might collude with an e-Government service operator or an external threat agent to commit fraud or gain access to protected information.

b) **Government users or their representatives** who are, or have been, responsible for the provision or operation of e-Government services may seek to exploit that privileged position. This will generally include government employees, their agents or employees of outside organisations contributing to e-Government services. Such individuals may possess significant resources and technical skills in addition to privileged access rights. Their motivation is likely to be fraud or personal dissatisfaction. Service operators are readily subject to sanction in the event that security breaches are traceable to them. Again, there is the potential for mistakes by government users or their representatives.

c) **Insiders** who are not associated with the provision of e-Government services but who may share access to the ESPD. This will generally include government employees or their agents who have access to the ESPD but no responsibility for e-Government service provision. These are individuals who are able to mount an attack from within the ESPD or TSPD and may possess a strong motivation to do so. Members of the ESPD will be readily subject to sanction; similar sanctions must be available for application within the TSPD. Again, there is the potential for mistakes by insiders.

4.2.2 External sources of threat

Some of the potential threat agents are outsiders and are beyond the control of the system authorities. These include:

---

[18]   It is envisaged that organisations where MPS applies will obtain such advice from the Security Service while other organisations (eg local authorities) would use CESG CLAS consultants.

a) **Hostile outsiders** are individuals or groups who possess access to the PND but no other association with the e-Government services. Such individuals may possess significant technical skills with a strong motivation to subvert the e-Government service provision, either for personal gain or other reasons. They may reside outside the government jurisdiction and not be subject to sanction or cessation orders.

b) **Criminal organisations** including organised crime groups as well as petty criminals may be attracted by the potential for large-scale fraud presented by e-Government services. Some IT related fraud is already known to have taken place.

c) **Foreign intelligence services** may seek to exploit e-Government services as a means of obtaining information on the workings of government or on individuals of interest. There may also be a threat of attacks designed to disrupt the workings of e-Government although such attacks are only thought to be likely in times of heightened international tension.

d) **Commercial organisations** may seek to acquire information about competing companies, customers, debtors *etc* from e-Government related sources.

e) **Investigation agencies** may seek to exploit e-Government systems as a source of information on targets of interest – for example financial information or other personal details.

f) **Terrorist organisations** may seek to exploit e-Government systems as a source of targeting information on individuals. In the future, there may be a threat of electronic attack designed to disrupt or bring down e-Government services.

4.3   Possible methods of attack

This section identifies the principal means by which the identified sources of threat may seek to attack e-Government services and systems. As with the sources of attack, regular updates of the current state to the threat arising from the application of such methods will be required[19] to ensure that the protective measures remain appropriate.

4.3.1   Electronic attack
This section lists methods of attack that seek to exploit directly technical features and properties of the IT systems and plant that support the e-Government services.

a) Hacking includes all attempts at unauthorised access to IT systems whether by insiders or from external sources. Methods include the exploitation of weaknesses in configuration or implementation, unauthorised use of access credentials, and internal breaches of operating procedures.

b) Malicious Software (including viruses) threatens the availability and integrity of IT systems. Specifically targeted introduced software may also threaten the privacy and confidentiality of stored information. The number of computer viruses in existence continues to rise. The

---

[19]   It is envisaged that organisations where MPS applies will obtain such advice from the Security Service while other organisations (eg local authorities) would use CESG CLAS consultants.

sophistication and potential for damage possessed by modern viruses is significant. Most viruses are now passed as attachments to e-mails but the risks posed by uncontrolled use of storage media or access to active content via a browser should not be discounted.

c) Denial of service flooding attacks are designed to render a target system temporarily unusable by overloading the external access points to the system with excessive numbers of requests for service.

4.3.2   Other attack approaches

This section lists those methods of attack that exploit indirectly the features of the IT systems supporting e-Government services. There are many attack approaches that involve the behaviour of clients and other users.

a) Insiders are well placed to circumvent security installations designed to prevent attack from outside. Use of an insider is the preferred method of attack for many hostile organisations.

b) Deception may be practised by sophisticated attackers who may attempt to pass themselves off as clients or other users in order to achieve access to information of interest. This is already practised widely in telephone transactions and the potential exists for similar attacks to be carried out by electronic means.

c) Denial may be practised by attackers who may attempt to deny a commitment or obligation entered into as part of an e-Government service action. If a legitimate transaction can subsequently be disavowed or otherwise challenged, opportunities for fraud are created.

d) Forgery may be used to create or obtain false access credentials and thereby gain unauthorised access to e-Government services.

e) Theft may be used to obtain unauthorised control of legitimate access credentials or other information or equipment, which may then be presented to gain unauthorised access to e-Government services.

4.4   Accidental damage

e-Government systems need to be protected against threats of accidental damage. Because occurrence of such incidents is, by their nature, difficult to predict, it is impossible to obtain a precise assessment of the impact of such threats. Protective measures should be in place to guard against the impact of such eventualities where justified by their likelihood and the potential damage. Some possible threats to be considered are listed below.

a) Inexpert clients or other users may unintentionally damage the e-Government service provision. Whilst such errors are unlikely to be motivated by an intention to undermine e-Government services, they may cause significant disruption or damage by, for example:

  i. unauthorised disclosure of information, for example personal information that could lead to fraud or undermine confidence in the system and could lead to legal action that might result in fines for the service provider;

ii.   failure to revoke client or other user rights, including those of staff working for third-party providers, once they are no longer required;

iii. loss of business information if, for example, access credentials are lost or the information is accidentally deleted.

b) Operators and administrators of e-Government systems may also, through incompetence or inadequate training, cause damage to the service assets or its continuing availability. Such individuals are not specifically motivated to undermine the systems but, owing to the privileged positions they hold, may unwittingly cause significant damage.

c) The introduction of leading edge e-Government services based on highly complex, new and unstable infrastructure may lead to suspension of the service or damage to the stored information base.

d) Inadvertent errors in the design, implementation and testing of the service by government employees or by third-party providers may lead to suspension of the service, damage to the stored information base or loss of confidence in the service. For example, inadvertent mis-sizing could lead to overload and thus denial of service.

e) Inadvertent introduction of erroneous information could undermine confidence in the system. For example, information on a central government or local authority web site could be factually incorrect.

f) Equipment or software failure may lead to suspension of the service or damage to the stored information base.

g) Accident or other disaster may destroy the service provision or the stored information base.

5. Security control objectives

5.1 Introduction

This section sets out a set of security control objectives that distil the threat, assets and environment assumptions. If these security control objectives are all met, they will ensure that the threats identified are properly countered in the declared environment.

5.2 Environment assumptions

The principal environment assumptions that relate to the provision of IT services are tabulated below.

Environment assumption	Notes
1 – Open Delivery	
e-Government services are delivered using a public infrastructure over which the business sponsors have little or no control.	The requirement is that no government special infrastructure is necessary to deliver the services. The Internet is seen as the delivery mechanism of choice though direct dial-in over the PSTN may be acceptable in special cases. No assumptions can be made about the assurance provided by any security mechanisms within the client workstation.
2 – Existing Secure Networks	
The systems hosting e-Government services are installed and managed in accordance with existing policy and practice for government systems connected to other networks.	A statement about the environment, which cross-references to existing codes of practice and policy on government and other service supplier data networks is required.
3 – Government Best Practice	
e-Government services must be implemented so as to conform to commonly understood 'best practice' and support the standards of probity that are expected of government actions.	A general statement is required that government typically sets standards for its own integrity and probity, which do not lay it open to challenge.

4 – Unassured Client Domain	
e-Government services must be implemented in a way that permits adequate trust relationships to be established between the participants without requiring strong controls or constraints on the terminals used to access the services.	Much of the equipment used by members of the public to access the services is typically uncontrolled and under non-technical management control that is unaware of security risks (*eg* a domestic PC). Government should not normally place constraints on the state of such equipment as a condition for e-Government service access, especially for services that do not require, for example, strong levels of registration and authentication. Security approaches will have to allow for this.
	The client is assumed to have a responsibility to ensure that any trusted elements (eg a Smartcard) are protected appropriately. The client needs to confirm his/her responsibilities as part of gaining access to the e-Government services.

5.3   Security control objectives

The security control objectives are necessarily high level and seek to minimise constraints on candidate implementations. Some of the objectives will be levied on the environment and will trace to security requirements that the environment must be shown to meet. The security objectives are those for the e-Government services themselves though not all are necessarily relevant to all services. The principal control objectives are tabulated below (cross-reference to BS7799 controls marked {BS x.y.z}. For BS7799 compliance, controls should be defined in terms of Part II Sections 4.1 to 4.10.

Service control objective	Notes
OS1 - Effective user identification & authentication	
Accountable e-Government services are accessible only to those individuals and systems that have been authorised to access such services. {BS: 4.7.2}	Will map on to a requirement for technical measures to ensure that access can only be obtained on presentation of properly constructed access credentials. Access is qualified as 'accountable' so as not to exclude some anonymous access (*eg* information only access).
OS2 - Effective user registration	
Access permission is granted only to those whose bona fides have been properly established. {BS: 4.7.2}	Will map on to a combination of technical and procedural measures to ensure that clients and other users are properly identified and authenticated before being granted access – a significant problem in public access systems – and that false or multiple real-world identities cannot be created. However, owing to the difficulties of achieving the latter, mechanisms also need to be put in place to identify multiple real-world identities.

Service control objective	Notes
OS3 - Effective access control	
Access granted to e-Government service applications and assets is the minimum necessary for the identified clients or other users to obtain the services required. {BS: 4.7.4}	Will map on to a requirement to ensure that a client or other user in whatever role, once identified and authenticated, can access only those parts of the system and assets necessary to perform the authorised task.
OS4 - Effective user access management	
Business sponsors exercise complete control over the access rights granted to e-Government service clients or other users. {BS: 4.8.3}	Will map to the requirement to install and remove user profiles as required – without the involvement of the client or other users. Technically this will map to requirements for access revocation for the specific service and, for example, certificate revocation schemes.
OS5 - Non repudiation	
Transactions are demonstrably traceable to the originator. {BS: 4.8.3}	Business sponsors must be confident that transactions enacted by an electronic or real-world identity can only have been carried out by that electronic or real-world identity. This frustrates attempted denial of responsibility for fraudulent use. Moreover, clients need to be assured that the service providers cannot repudiate the service provider's part of a transaction. Equally service providers might wish to be assured that government cannot repudiate its part in a transaction either.
OS6 - Evidence of receipt	
Transactions are demonstrably traceable to the recipient. {BS: 4.8.3}	Clients and other users (including service providers) of the services must be able to demonstrate that transactions submitted have actually completed and that they cannot be falsely accused of failure to submit required returns or deny receipt of information.
OS7 - Trusted commitment service	
Any commitments made using e-Government services are not liable to theft or fraud. {BS: 4.8.3}	Authorised clients of e-Government services must be confident that (for example) their authorities for payment will be properly controlled and are not vulnerable to fraudulent use of their means of payment, subject to the clients keeping relevant credentials or other personal information secure.
OS8 - Privacy and confidentiality	
Personal and other information submitted to services is not disclosed or visible beyond those authorised and with a need to receive it. {BS: 4.8.3}	Personal details submitted by a client of e-Government services must be properly protected in accordance with the DPA at all times within the e-Government service. Internally, within the service provider, information must be handled responsibly and securely. This includes the concept that the real-world identity should be kept confidential for some e-Government services (eg reporting of fraud or criminal activities).

Service control objective	Notes
OS9 - Integrity	
Information received from or passed via the services is not altered or otherwise subverted. {BS: 4.8.3}	Clients or other users of e-Government services must be confident in the correctness, completeness, and authority of information and advice received in an e-Government service transaction and that anything they submit will be correctly received. This covers both erroneous information and information inadvertently or maliciously altered during storage, processing or transit.
OS10 - Service availability	
Continuing access to the service as and when required must be assured. {BS: 4.9.1}	Clients and other users of the e-Government service must be able to depend on the continuing availability of the service to meet their obligations with respect to government service provision – subject to limits imposed by the availability of the PND.
OS11 - Information availability	
Continued access to the e-Government data assets as and when required must be assured. {BS: 4.9.1}	Data assets of the e-Government service are an important record and must not be lost through accidental, careless or deliberate acts of e-Government service clients or other users, or in the event of equipment failure.
OS12 - Service protection	
The e-Government service implementation and associated assets must be protected against outside interference and penetration. {BS: 4.2.2}	The e-Government services must be adequately protected from outside attack mounted against the service applications themselves or the underlying network infrastructure.
OS13 - Effective audit and accounting	
The e-Government service must keep a proper record of significant transactions. {BS: 4.10.3}	There is a general requirement for a proper record of significant events that may have to be revisited. This is required partly to meet external audit requirements, and partly as a mechanism for making clients and other users accountable. It includes appropriate records to demonstrate that privacy and confidentiality have been maintained.

5.4   Relationship to other security framework documents

The means of achieving these security control objectives are considered in detail in other framework documents as described below. The documents form a complete set and it is strongly suggested that they should be read together.

This document 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[20] document addresses the following objectives:

h) OS1 – Effective user identification and authentication;

i) OS2 – Effective user registration;

j) OS3 – Effective access control;

k) OS4 – Effective user access management.

The trust services framework document[21] 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[22] addresses the following objective:

a. OS8 – Privacy and confidentiality.

The business services framework document[23] addresses the following objectives:

b. OS10 – Service availability;

c. OS11 – Information availability;

d. OS13 – Effective audit and accounting.

The network defence framework document[24] addresses the following objective:

a. OS12 – Service protection.

---

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

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

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

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

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

The assurance framework[25] document addresses the means by which trust in the implementation of security elements can be assured.

---

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

6. Service functional security requirements

The service control objectives may be met by ensuring that the following functional security requirements are met by any proposed installation. These security requirements are, as far as possible, independent of specific techniques and technologies used to satisfy the security requirements. However, the need to provide a universal service requires that some technical choices be made at the security requirements level in order to secure interoperability.

For convenience, the security requirements are categorised by the primary security objective of the requirement. The additional rationale provides greater detail on these relationships in order to demonstrate completeness.

OS1 – Effective user identification and authentication	
1.1 User access to accountable e-Government government services shall be granted to authorised users only.	The standard identification and authentication requirement is to limit access only to those who have been properly identified and authenticated.
1.2 User access privileges granted to e-Government services shall be the minimum necessary to satisfy the business requirement for that service or management function.	A standard privilege minimisation requirement to limit the potential for damage caused by authorised users. This includes separation of service user and administrative roles.
1.3 It is desirable that user access to accountable e-Government services shall be conditional upon the presentation of an access token issued by or on behalf of government service providers.	Access control can be made stronger through the use of properly designed access tokens. There is a strong preference for these to be used though there may be circumstances where the risks are low enough for tokens to be unnecessary.
1.4 User access to e-Government services shall require the presentation of authentication credentials and supporting information to identify the individual requesting access.	An implementation requirement for personal authentication beyond possession of the token. The type of personal authentication is not specified but will probably be a password unless biometrics is permitted.

OS2 – Effective user registration	
2.1 Access rights to e-Government services shall be granted only when e-Government service management or their agents are satisfied that the user is actually who he/she claims to be, is not already registered under a different real-world identity, and has a legitimate need for access.	A requirement to prevent impersonation or the issue of access rights to bogus individuals or the creation of multiple real-world identities that could be misused. An individual may possess multiple roles with respect to e-Government services but can only ever possess a single real-world identity. HMG has published guidelines for the verification of the identity of individuals[26] and organisations[27] that describe how this can be achieved.
OS3 – Effective access control	
3.1 User access shall be possible only to those e-Government system services and/or assets, which are necessary to support the specific service requested.	A requirement to enforce internal access controls at the object or application level such that a legitimate user, once granted system access, cannot influence or damage system data which the required service does not need.
OS4 – Effective user access management	
4.1 The possession and issue of user access rights shall at all times be under the control of system management.	General requirement for a management framework for user access rights.
4.2 It shall be possible for system management to revoke a user's access rights in a timely fashion without the presence or involvement of the user involved.	Specific requirement to be able to revoke a user's rights and without reference to or permission of him/her. Any access credentials and or tokens cease to have any validity. It is recognised that immediacy may not be feasible; the aim should be for the revocation to take place as soon as possible bearing in mind the risks of misuse in the intervening period.
OS5 – Non repudiation	
5.1 The e-Government service shall provide evidence that a transaction received from an authorised user did actually originate from that user who cannot subsequently deny responsibility for the transaction.	Requirement to provide a binding between transactions purporting to come from a user and actions of that user in person identified by an electronic or real-world identity. The system should have some means of preventing a user subsequently denying responsibility for a transaction, or third parties falsifying a transaction that purports to come from a user.

---

[26]   *e-Government strategy framework policy and guidelines HMG's minimum requirements for the verification of the identity of individuals (Under revision following public consultation)*

[27]   *e-Government strategy framework policy and guidelines HMG's minimum requirements for the verification of the identity of organisations (Under revision following public consultation)*

OS5 – Non repudiation (continued)	
5.2 The e-Government service shall provide evidence as to whether a transaction received or claimed to have been received by a user did actually originate from the e-Government service.	Requirement to provide a binding between transactions received from an e-Government system and the actions of the system. The system should have some means of verifying the authenticity of information from the system and preventing users disputing the authenticity of information received, or claimed to have been received. This also includes the access system.
5.3 The e-Government service shall provide evidence that information received from a user was actually submitted by that user and the service cannot dispute the authenticity of the information.	Requirement to provide a binding between transactions from a user and the receipt of that information into the service. The user wishes to be assured that he can prevent the e-Government service disputing the authenticity of information received. The strength and type of evidence needs to be commensurate with the service being provided.
5.4 The e-Government service shall provide evidence that the service is indeed provided officially by, or on behalf of, a central or local government organisation.	Requirement for an access system to establish a credential and present this to the client for authentication of the access system to the client.
OS6 – Evidence of receipt	
6.1 The e-Government service shall provide evidence that a transaction received from a user was accepted by the service and receipt cannot subsequently be denied by the service.	Requirement to provide a strong receipting mechanism to users such that, in the event of a dispute, users are able to make a strong case that they have met their obligations with respect to the service provision.
6.2 The e-Government service shall provide evidence as to whether a transaction dispatched to a user was actually received by that user and receipt cannot be denied by the user.	Requirement to provide a strong receipting mechanism to the system such that, in the event of a dispute, system management is able to make a strong case that information apparently received by a user was actually received. The system should have some means of preventing a user falsely denying receipt of information or notice of required action.
OS7 – Trusted commitment service	
7.1 The e-Government service shall protect instruments of commitment from fraudulent use or other exploitation.	Requirement to provide assurance that exploitable user payment authorities (such as credit card information) or other commitment vehicles are properly protected by the service. There may be a need to demonstrate this protection in the event of a dispute.
7.2 The e-Government service shall provide auditable receipts for all commitments made with or via the service.	Requirement to provide proper evidence of commitments made and received such that, in the event of a dispute, it is possible to demonstrate, for example, a payment history to an external auditor.

OS8 – Privacy and confidentiality	
8.1 The e-Government service shall provide adequate protection of personal and private information from observation or disclosure when in transit across vulnerable network segments.	A requirement to review the need for communications confidentiality. This is as required to meet obligations under privacy and data protection legislation. The measures should be appropriate for the threat and seek to deny access to all those not authorised.
8.2 In accordance with the Data Protection Act, the e-Government service shall protect personal and private information from misuse when stored and processed within the e-Government service implementation domain.	A requirement to meet privacy and data protection obligations within the ESPD. This will require the service operators to demonstrate best practice and fulfil their legal obligations with respect to personal data. Note that personal information that is stored within the client domain is a client responsibility.
OS9 – Integrity	
9.1 The e-Government service shall protect information transmitted across public networks from exploitation by accidental or deliberate modification, deletion or replay.	A requirement for strong communications integrity measures to prevent an attacker from manipulating the data in transit or from loss and corruption caused by equipment or communications failures.
9.2 The e-Government service shall protect service information stored within the unassured client domain from exploitation by accidental or deliberate modification.	A requirement for storage integrity measures in the client workstation. This will prevent the user or other attacker from manipulating the stored context on the workstation in order to gain some advantage. A requirement to protect against unintended corruption will be met if deliberate corruption is controlled. Note that this is not intended to reduce the ability for a user to amend personal details stored locally. It relates to application data (*eg* cookies) that is stored locally but is under service ownership – for example stored context between application sessions.
9.3 The e-Government service shall protect information stored within the e-Government service implementation from deliberate modification or destruction by outside attackers.	A requirement for strong measures to frustrate 'hacking' attacks on the service that might undermine confidence in the service by maliciously altering user data or publicly posted information (*eg* modifying web pages). The e-Government service provider also has a duty of care to ensure that information provided to clients is not erroneous.
9.4 The e-Government service shall protect information stored or transferred within the e-Government service implementation domain from accidental loss or corruption.	A requirement for 'best practice' integrity measures within the service. Electronic signature based measures can be used where possible but it is probably adequate (and more readily implemented) to rely on standard access control techniques. This will also lead to requirements to implement tested recovery procedures and to ensure that lists of authorised clients and users are maintained.

OS10 – Service availability	
10.1 The e-Government service shall be protected against outside attack, which seeks to damage or deny provision of the service to authorised users.	A requirement for strong security measures to prevent the service being susceptible to external denial of service attacks.
10.2 The e-Government service shall be protected against internal equipment failure, which might damage or prevent continuing provision of the service.	A requirement for best practice design approaches to prevent the service being unduly susceptible to failure following equipment failure. Will require a measure of redundancy consistent with the importance of continued service provision and the ability to effect swift repairs.
10.3 The e-Government service shall be protected against loss of data, loss of equipment, and other external adverse events.	A requirement for a business continuity plan and supporting measures. There is a general requirement to anticipate disasters and make sure that the necessary measures are instituted to avert disaster where possible and recover where prevention is not an option.
OS11 – Information availability	
11.1 The e-Government service shall make provision for the retrieval of critical or personal data that has been damaged or destroyed by malicious or other actions.	This is a business continuity requirement for a proper backup regime to ensure that the active datasets are secured and can be restored in the event of failure.
11.2 The e-Government service shall make provision for retrieval of protected information in the event that a client or other user is unable to supply the necessary access credentials.	This is a business continuity requirement to provide facilities to recover user data in the event that an access token or password is lost. This facility may also be required to support investigations of possible system misuse where the suspects might be alerted by requesting their credentials.
OS12 – Service protection	
12.1 The e-Government service application and underlying network infrastructure shall be protected against outside attack that seeks to undermine continued service provision.	Any system that is connected to public networks is open to attack by those seeking to damage or deface the service without necessarily seeking personal gain. The underlying networks must be hardened against such attack using measures such as boundary control and scanning devices. The applications themselves must be constructed in such a way that vulnerability to outside attack is reduced to an acceptable level.
OS13 – Effective audit and accounting	
13.1 The e-Government service application shall maintain a record of transactions that may require after the event analysis.	General requirement for maintenance of audit and accounting logs. Reasons for requiring this include establishing accountability for transactions, reconstructing failed transactions and furnishing appropriate records in the event of a dispute about services. Each record should be traceable to a real-world or electronic identity, where appropriate.

A   Glossary

The following definitions align with those set out in related security framework documents.

A.1.1   Access system

An access system is an IT system that in conjunction with one or more back-office systems hosts e-Government services. Clients gain access to e-Government services via an access system element. Examples of access systems are the Government Secure Internet (GSI) and the government gateway.

A.1.2   Access system registration

Access system registration is the process in which an access system can establish a credential and present this to the client for authentication of the access system to the client.

A.1.3   Access token

An access token is a (physical) medium that contains a credential, for example a smartcard that contains a digital certificate.

A.1.4   Accreditor

The person responsible for the accreditation of a system or service.

A.1.5   Anonymous client

An anonymous client is one who chooses to reveal no real-world identity during the registration process prior to authentication for a specific transaction. The client may or may not possess a credential. A client possessing a credential, with an associated electronic identity, can be recognised for repeat transactions using that credential. If the client does not need to possess a credential, any resulting transactions could be truly anonymous and untraceable.

A.1.6   Assurance

Assurance is the set of processes and practices to help ensure that e-government services are designed, implemented, configured, maintained and operated in accordance with the security framework.

A.1.7   Assurance level

The assurance level is a measure of assurance matched to security profile defined by the Common Criteria for IT Security Evaluation. This should comply with ITSEC or *tScheme* approval.

A.1.8   Authentication

Authentication is the process by which the electronic identity of a user is asserted to, and validated by, an information system for a specific occasion using a credential issued following a registration process. It may also involve establishing that the user is the true holder of that credential, by means of a password or biometric. A client is required to authenticate their electronic identity every time they wish to engage in an UKonline session.

A.1.9   Authorisation

Authorisation is the granting of rights to access services, information and resources.

A.1.10 Back-office system

A back-office system is the computer system within a government department, agency, local or regional authority or other e-government service provider, which completes a requested service based on data passed from an access system.

A.1.11 Business sponsor

The individual within the government organisation that holds overall responsibility for the service provision and security of an e-government service. The business sponsor works in conjunction with the service provider (who may or may not belong to the same organisation) and accreditor to select, implement and assure appropriate security measures for the service.

A.1.12 Certificate Revocation List (CRL)

A certificate revocation list is a list of certificates that have been withdrawn prior to their normal expiry date.

A.1.13 Certification Authority (CA)

A certification authority issues, manages and revokes digital certificates at the request of Registration Authorities.

A.1.14 Challenge response

Challenge response is a mechanism that is typically used to test whether the recipient of the challenge can be authenticated for a particular service. It can be implemented using PKI techniques.

A.1.15 Client

A client is a person, an organisation, a duly authorised representative of the person or organisation or a process seeking to carry out a transaction with government.

A.1.16 Credential

A credential is a set of information, which is used by a user to establish an electronic identity to a computer system as part of the authentication process. A credential may be associated with ancillary information supporting a client's right to possess that credential (such as a PIN or private signing key). Examples of credentials are client identifiers or a digital certificate held within a smartcard.

A.1.17 Credential issuer

A credential issuer issues, manages and revokes credentials. A Certification Authority is one example of a credential issuer.

A.1.18 Credential revocation list

A credential revocation list is a list of credentials that have been withdrawn prior to their normal expiry date.

A.1.19 Directory

A directory is the set of information that allows an access system to map uniquely between the client's credential and the information (in database terms, the 'primary key') needed to identify the client to the service the client is requesting.

A.1.20 Disenrolment

The process by which a client's right to a particular service is removed.

A.1.21 Electronic identity

An electronic identity is a set of information that uniquely identifies a user to a computer system. Examples of an electronic identity are a username or digital certificate identifier.

A.1.22 Enrolment

Enrolment is the process by which a client obtains authorisation for a specific online service.

A.1.23 Government gateway

The government gateway is a specific example of an access system. It is a hub linking portals and external back-office systems to government back-office systems. Amongst other things, the gateway provides common security services, including client authentication, confidentiality and privacy. Once a client has been authenticated, the government gateway forwards information between the client and appropriate government back-office systems. It co-ordinates transactions on government back-office systems on behalf of the client to support 'joined-up' government services. The government gateway also provides a secure messaging facility to allow government departments to communicate with the client. The linkage between a portal and a government back-office system may be asynchronous, or synchronous.

A.1.24 Government gateway enrolment

Enrolment at the government gateway is the process by which a client first registers with a relevant access system by presenting an acceptable credential. The access system will check the validity of the credential and set up a directory entry corresponding to the credential and containing information specific to the client.

A.1.25 Government user

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

A.1.26 Practice statement

A practice statement is a statement, published by a registration service provider or a credential issuer, setting out its practices in registering clients and issuing and managing credentials.

A.1.27 Pseudonymous client

A pseudonymous client is one who chooses only to reveal a pseudonym as part of the registration process prior to authentication for a specific service. The client may or may not possess a credential. A client possessing a credential, with an associated electronic identity can be recognised for repeat transactions using that credential. If the client does not need to possess a credential, any resulting transactions could be truly pseudonymous and untraceable.

A.1.28 Real-world identity

A real-world identity is a set of attributes (*eg* name, date of birth, national insurance number), which uniquely discriminates between users. An entity can possess only

one real-world identity (*eg* a person or an organisation). However, a single real-world identity may be used in conjunction with different roles. Depending on the transaction, a user may be required to reveal their real-world identity or may be permitted to use a pseudonym or remain anonymous.

A.1.29 Receipt

A receipt provides evidence for a party in a transaction that can be used at a later date to confirm that a specific element of the transaction has been completed.

A.1.30 Registration

Registration is the process by which a user gains a credential such as a username or digital certificate for subsequent authentication. This may require the client to present proof of real-world identity (such as birth certificate, passport) and/or proof of other attributes depending on the intended use of the credential (*eg* proof that an individual works for a particular organisation). Registration can be associated with a real-world identity or can be anonymous or pseudonymous.

A.1.31 Registration Authority

A registration authority (RA) is the organisation that validates evidence both of a user's real-world identity and of the client's right to that real-world identity. If the identification is successful, the client will usually be supplied with a credential for subsequent authentication (either directly, if the RA is also a credential issuer, or by another body such as a certification authority).

A.1.32 Registrant

A registrant is a person, an organisation or representative of a person or an organisation seeking to establish their identity and obtain a credential from an issuer.

A.1.33 Registration and enrolment policy

It is envisaged that there would be a detailed registration and enrolment policy statement for access systems that provide client access. This would include, for example, the clients entitled to register, the appropriate type of registration for each UKonline service, information that needs to be collected from a client during registration and enrolment, the appeals process, acceptable credentials and the relationship between a credential provider and the government.

A.1.34 Relying Party

The relying party trusts a credential to associate an electronic identity with a client. The relying party is often the organisation that is responsible for carrying out the government service, and hence relies upon a credential as part of authorising a

client. For example, the Inland Revenue is the relying party for a client's Income Tax Self-Assessment. However, clients may also be relying parties if they rely on a government credential to assure themselves that they are really dealing with government.

A.1.35 Risk

Risk is a function of asset value and the impact and likelihood of threat and vulnerabilities.

A.1.36 Risk assessment

A risk assessment is an assessment of threats to, impact on and vulnerabilities of information and information processes and the likelihood of their occurrence.

A.1.37 Roles

A client may assume one or more roles in the client's interaction with government. For example, a person may simultaneously be both an employee and an employer. Similarly, government users may assume a number of roles in their interaction with e-government services.

A.1.38 Security domain

A security domain is a set of equipments or security processes within a specific management regime.

A.1.39 Service provider

The service provider is an organisation responsible for the provision of a specific e-government service. The service provider might merely operate the service using its own or government-owned equipment, or it might also design and develop the service.

The service provider must ensure that the service and relevant systems are compliant with the e-government security framework, in conjunction with the accreditor and the business sponsor.

A.1.40 Threat

A threat is the likelihood that an attacker will attempt and has the capability to exploit a vulnerability to breach security.

A.1.41 Trust service provider

A trust service provider is an organisation that provides trust services. Trust service providers include registration authorities, since they provide a measure of trust in the asserted real-world identity of a client.

A.1.42 UKonline

As a brand, UKonline refers to the provision of government services by electronic means. The service provider could be, for example, one or more of a central government department, a government agency, a local authority or a private sector organisation acting on behalf of local or central government.

A.1.43 UKonline citizen portal

The UKonline citizen portal is the current electronic interface between clients and the government. It is accessed through Internet-based technologies, uses websites to bring information together and a gateway to provide a common interface to the government back-office systems operated by government departments and agencies. The UKonline citizen portal also presents publicly available information. The UKonline citizen portal is one of a number of portals that provide access to UKonline services.

A.1.44 UKonline service

A UKonline service is any service that a client can access electronically within the UKonline brand.

A.1.45 Unpublished data

Unpublished data is information that is likely to be known only to the credential holder and the service provider: for example, information about a previous transaction.

A.1.46 User

A user is a person or process that interacts with an e-government system (in any capacity).

A.1.47 Vulnerability

A vulnerability is a feature of a system which, if exploited by an attacker, would enable the attacker to breach security.

B   Abbreviations

CPS	Crown Prosecution Service
CC	Common (evaluation) Criteria
CND	Client Network Domain
CSSD	Client Side Service Domain
DPA	Data Protection Act
DSPD	Departmental Service Provision Domain
eGIF	e-Government Interoperability Framework
ESPD	e-Government Service Provision Domain
GSI	Government Secure Internet
NDSPD	Non-Departmental Service Provision Domain
PC	Personal Computer
PKI	Public Key Infrastructure
PND	Public Network Domain
PP	Protection Profile
TSPD	Trusted Service Provider Domain

C   Example e-Government service scenarios

This annex presents some representative scenarios to which the government service delivery security requirements might be applicable. The list is not intended to be exhaustive and is presented for discussion. These are examples only and do not imply any intent or commitment to offer such a service, nor are the analyses of the scenarios intended to be complete.

Scenario 1 – Single department transaction

A member of the public or a business wishes to carry out a service transaction with a single government department. The service has monetary and/or utility value. He/she accesses the 'service entry page' for the service on the Web. He/she completes an electronic form, signs it electronically as affirmation of his/her real-world identity and attaches any other certificates or documents necessary and submits the form. If appropriate, he/she authorises payment of the fee. The department actions the form and confirms with a dated and signed receipt either along with, or to be followed by, the deliverables of the service in question.

Examples include application for benefit, grant, licence, certificate of approval, and registration of status or search of registration information, passport issue, tax assessment and coding.

Scenario 2 – Multiple department transaction

As scenario 1 but the transaction involves more than one department. In this case, the transaction requires action by multiple departments and the co-ordination of responses.

Examples include arranging long-term domiciliary care for the individual and business transactions such as arranging development grants, export credit guarantees, company registration details and returns, and VAT/PAYE/National Insurance.

Scenario 3 – Private correspondence with government

A professional (consulting engineer, barrister, *etc*) wishes to correspond with an official in a government department, via electronic media with a guarantee of confidentiality at least as good as conventional methods of communication.

Examples include members of the bar corresponding with the Crown Prosecution Service (CPS) on briefs, and consultants or suppliers acting on procurements.

Scenario 4 – Change of personal status

A member of the public changes some personal details. He/she is able to access a service, which will capture the details of the change (when bona fides have been established) and communicate it to interested government departments. Confirmations are made available to the client.

Examples include change of name, home address, e-mail address, phone number, marital status and death.

Scenario 5 – Employment application

A job seeker browses vacancies using one of many electronic transmission media (Web, kiosk, interactive television, e-mail subscription list). He/she applies and (when he/she has provided proof of his/her real-world identity) his/her CV is automatically called up if he/she has one stored. He/she has the opportunity to add modify or delete details.

If there was not a CV stored, he/she is invited to create one. He/she lists referees and contacts them to make sure they are happy to speak for him/her. He/she calls up certified qualification details by submitting a request to the relevant academic institution(s). Then he/she approves the application to be forwarded to the prospective employer. He/she gets a receipt from the employer either with or to be followed by notification of the results of the application.

Scenario 6 – Information search

A member of the public browses public information provided by government and possibly enters into some commitment on the basis of the information obtained.

Examples include Foreign Office travel information (leading to some travel commitment), DTI business information (possibly leading to some contractual commitment).

Scenario 7 – Purchase of government information

A member of the public or a business queries a department for specific information. The client provides contact information and pays a fee if appropriate.

Examples include purchasing documents or information relating to policy formulation, historical information, or legal obligations.

Scenario 8 – Electronic voting

A member of the public registers their intention to vote electronically in an election. He establishes his bona fides and this is checked against the voters' list and he is given an electronic ballot paper for the constituency in question. Between the times the electronic ballot box opens and closes he chooses his candidate and submits his vote. When the ballot closes, votes are scrutinised and counted, and the electronic count conveyed to the returning officer, for consolidation with the manual count.

Scenario 9 – Interdepartmental request

A member of a Government Department service team has to deal with a query related to an application made via a 'portal form' for a 'joined-up' service. They are logged in on their computer terminal so they can call up relevant data from other departments, agencies and local Government who are involved in the case as notified on the original submission. The details are checked and contact is made with other case officers whose details were discovered in this search. A response is then sent to the applicant and the other officers notified.

Scenario 10 – Granting permission to access services

A member of the public wishes to access government services electronically for the first time. He applies for access and is given an appointment with an approved agent to establish his bona fides, and is then given the means to obtain access.

Scenario 11 – Enrolment of government employee

A new recruit to a Government Department arrives for the first day at work. They are brought onto the Departmental 'roll' and given the means to identify themselves electronically as a member of the Department.

Scenario 12 – Fraud investigation

A government employee or agent is suspected of acting in a fraudulent or corrupt manner in association with partners outside government with whom he is in electronic communication. An investigation is launched which may require access to his transaction record without informing him.

Scenario 13 – Revocation of government employee

A government employee or agent is suspended or resigns and their authorities relating to their post are revoked.

Scenario 14 – Access to e-Government services under delegated authority

A member of the public accesses an e-Government service on behalf of another individual, who is unable to access the service directly owing to disability etc. This would normally be under a power of attorney.

As an alternative, a member of a professional services firm (eg accountant, lawyer) wishes to submit formal documents on behalf of a client.

D   Model for security requirements expression

This framework document uses the internationally recognised Common (evaluation) Criteria (CC) Protection Profile (PP) model as the vehicle for the definition of security requirements[28]. The CC PP construct is defined for the expression of security requirements for an IT security product or system that is intended to be the subject of formal evaluation against the CC leading to certification of compliance with the PP security requirements. This document defines the security requirements for a service rather than a product, the CC definition of the PP construct has therefore been adapted to describe a secure service whilst maintaining as far as possible the underlying CC model.

The CC Protection Profile is a structured representation of security requirements that can be certified as a suitable response to the security problem described. Part 1 of the CC explains the underlying model in some depth; Figure D-1 below illustrates the PP concept.

The Protection Profile presents the security requirements in terms of the following:

a) The Security Environment is a statement of the security problem by identifying the assets, which are to be protected, the threat agents who might represent a threat to those assets, and the specific threats to those assets. A threat is a particular attack that exploits asset vulnerability.

b) The Security Objectives are a concise statement of a set of control objectives which, when achieved, will result in the required level of protection being achieved.

c) The Security Requirements are a set of technical security requirements statements against which any implementation can be tested.

The aim of the profile model is that it should be possible to show proper traceability from the environment (statement of the problem) to the objectives and thence to the detailed security requirements statements. The profile will be supported by a rationale that demonstrates that the security requirements are a complete, effective and cohesive solution to the security problem described.

This framework document currently makes no reference to the CC part 2 security components and packages. Security requirements are expressed in narrative form. Any adaptation to the needs of the evaluation community has been deferred until the principles and narrative content have been adopted as the basis for service provision and the detailed security requirements for the major elements of the security services have been determined.

---

[28]   Information on the CC project can be found at www.cesg.gov.uk/assurance/iacs/itsec/index.htm.
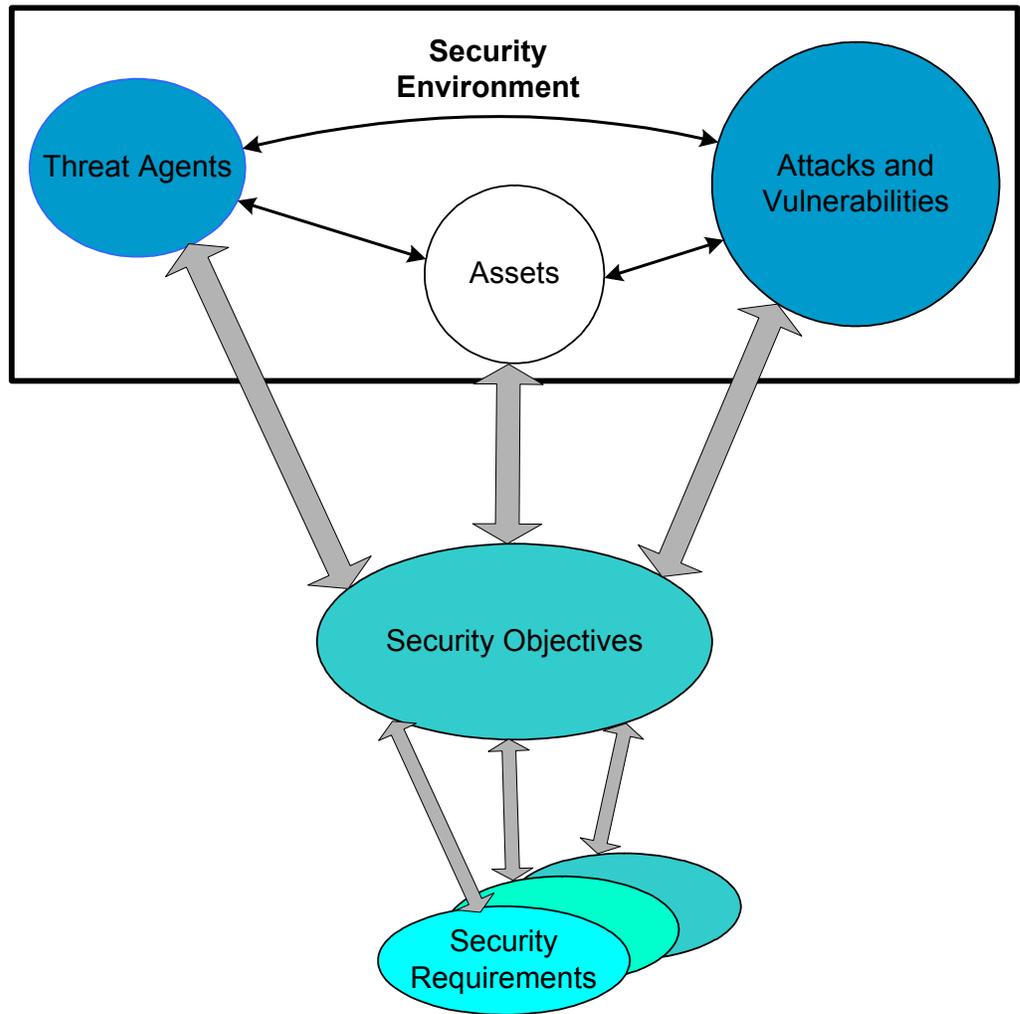
Figure D-1: Simplified Common Criteria Protection Profile Structure

E   Example e-Government service attacks and threats

This annex presents a starting point for the security risk analysis of threats to e-Government service delivery with reference to the assets and threat agents identified.

In considering whether a particular service offering might need to deal with such a threat, the actual risk of attack needs to be considered. If the asset value is low, the impact small, or the technical difficulty of mounting the attack is high, it may not be necessary to install specific countermeasures.

Threat	Notes
T1 – Unknown Outsider Attack	
A hostile outsider may gain direct access to e-Government services with the objective of achieving some personal gain or causing damage to the system.	This is the generally accepted 'hacker' attack from outside seeking to commit fraud or disruption. Examples might include fraudulently altering information held to the detriment of other transactions or the continuing provision of the service.
T2 – User Fraud	
A legitimate user or other client of e-Government services may submit a false transaction or deny obligations in respect of transactions submitted.	This is the generally accepted threat arising from dishonest clients or other users. An individual may have been legitimately granted rights to use the system and tries to abuse that position. In most cases, measures against this sort of threat are more of a business process / application requirement than a security requirement. Examples might include submitting multiple benefit claims and/or denying responsibility for fraudulent claims submitted and subsequently detected.
T3 – Insider Attack	
An individual with privileged access to government data networks may abuse that position to create false transactions or interfere with legitimate transactions.	This is the generally accepted 'insider' attack from other parts of government not directly connected with the service. Examples might include 'hacking' attacks from inside government networks on the more privileged inter departmental elements of the services. Note that the attack may actually originate from outside following a breach of the defences to the ESPD.
T4 – Privileged Insider Attack	
An individual with privileged access to, or management responsibility for, e-Government service provision may abuse that position to interfere with or exploit service provision.	This is the generally accepted 'insider' attack from operational staff responsible for the system. Examples are the traditional fraudulent use of privileged capabilities to alter records, create false accounting trails or create phantom users.

Threat	Notes
T5 – False Identity	
An individual may establish false or multiple real-world identities to access e-Government services and submit fraudulent claims or cause other damage to the service.	All classes of threat agent may have an interest in creating false real-world identities; insiders may find it easier than outsiders but are at greater risk. Example exploitations might include submitting benefit claims using false bona fides.
T6 – Impersonation	
An individual may impersonate a legitimate client or other user or operator in order to secure services on that user's behalf.	An individual may attempt to impersonate a client or other user, by forging or otherwise acquiring legitimate credentials and making representations on behalf of the legitimate user, which might be difficult to disavow.
T7 – Unauthorised Disclosure	
Personal information or other information submitted as part of an e-Government transaction may be disclosed to those with no need or rights to access it.	This is the generally accepted privacy or confidentiality threat. This could lead to a failure to comply with the DPA or the risk that the personal information gained could be used for fraudulent purposes and also undermine confidence in the service. Examples include the probing of the external networks for exploitable information such as payment credentials or personal information.
T8 – Revoked Rights	
Those who have in the past possessed rights of access to e-Government resources may misuse those rights after they have, or should have been, revoked.	This is the threat arising out of the inability to ensure that user rights are properly terminated once they are no longer needed. Examples might include misuse of the access rights of a deceased person or misuse of insider rights after the individual concerned no longer has the responsibilities that carry those rights.
T9 – Theft of Access Tokens	
Access tokens that confer rights with respect to e-Government services may be stolen and used for improper purposes.	Should some form of access token be used to control access, there is a threat that lost tokens might be abused. Examples might include theft of tokens or information required to gain e-Government access or validate transactions.
T10 – Duplication of Access Tokens	
Access tokens that confer rights with respect to e-Government services may be duplicated and copies used for improper purposes.	There is a distinct threat from loss of tokens in that a token holder may be unaware that the token has been copied. Examples include forgery or attempted copying of authentication tokens.

Threat	Notes
T11 – Capture of Access Credentials	
Access credentials may be captured and used for improper purposes.	Here the term access credential refers to the information needed to gain access rather than any token, which is the physical packaging of the credentials. There are several attack approaches that might achieve this including: - Passive monitoring of the network and other communications channels in order to acquire the authentication transfers and determine the authentication credentials. - Creation of a bogus e-Government access point with the intention of deceiving an unwitting e-Government access user into revealing genuine access credentials and other information. Subverting the CND such that access credentials or other transaction material might be disclosed to the attacker.
T12 – Denial of Service Attacks	
Threat agents may seek to deny access to the e-Government services by legitimate users.	This is typically a threat arising from external or internal attack – 'hacking' or 'cyber vandalism'. There are several attack approaches that might achieve that including flooding attacks that seek to stress the service, and attacks on the PND or ESPD, which might prevent legitimate transactions from being properly routed to the service.
T13 – Misinformation and Propaganda	
e-Government services, and hence use of the service, may be undermined by laying a trail of false and misinformation which purports to carry the authority of government by virtue of its apparent association with the e-Government service.	This is a threat arising out of an attack on the integrity of information held within or issued by e-Government with the aim of destroying confidence in the service. Examples might include the replacement of content of web pages with false information, or the alteration of purported origin, content or authority of communications from e-Government service providers.
T14 – Breach of Anonymity	
Transactions that are required to be anonymous may be traced to their originator and the association misused.	The primary example of this would be any use of e-Government systems for services such as ballots or informer lines where anonymity of the transaction is required.
T15 – Breach of Accountability	
Clients or other users of e-Government services, and the departments offering the services, may not be able to be held accountable for attempted fraud or maladministration.	A secondary consequence of a directed attack or fraud is that the system authorities may not know that such a fraud is taking place or what the extent is. Partially a business rather than security requirement, but security requirements will affect the protection of raw audit information.

Threat	Notes
T16 – Failure to Recover Business Information	
Information assets contained within the system may become inaccessible if the access credentials are lost or unobtainable.	Information may be lost following equipment failure or malicious attack. A proper backup regime will permit recovery from such situations.

Another concern here is where encryption is used as a mechanism to limit access to specific individuals and the access credentials are lost (*eg* the individual loses or forgets the key/password). In the absence of a proper business information recovery mechanism, the information asset could be lost. |
T17 – Loss or Theft of Monetary Value	
Monetary value owned by e-Government systems may be improperly disbursed.	This is a specific case of the generic threat of loss of assets where the assets represent monetary value. Financial accountability and control introduces extra requirements beyond the business needs to control information in general.
T18 – Challenge to System Veracity	
It is possible that a user may disavow a transaction with a claim that the e-Government system was imperfect.	There is a general requirement to be able to show that systems are correctly installed and operated and that any records generated by the system in support of a dispute are admissible and able to provide a sufficient weight of proof.