July 2010
Issue No: 1.0

Requirements for Secure Delivery of Online Public Services
Part 2: Security Components

CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Requirements for Secure Delivery of Online Public Services
Part 2: Security Components

Issue No: 1.0
July 2010

Requirements for Secure Delivery of Online Public Services
Part 2 - Components

Intended Readership

The intended readership of this document is those responsible for provision of online public services from their inception through to delivery and operation. It is of particular relevance to those responsible for service and system security including procurement and provisioning, accreditation, and security management.

It is, by intent, UNCLASSIFIED, and is intended to be available to all with a wider interest in the provision of government ICT services.

Executive Summary

Requirements for Secure Delivery of Online Public Services (RSDOPS), is a response to the challenge of delivering online public services to the citizen and sets out a proposed approach to deriving and agreeing security requirements for systems delivering public services electronically.

It revises, repositions, and will replace the E-Government Security Framework (e-GSF) last updated in 2002 (Ref [a]). The document is in 2 separate volumes. Part 1 (Principles) describes the scope, context and the approach to be followed in determining security requirements for future public service systems. Part 2 (Security Components), this part, describes the security components that are used to express the security requirements. Readers are assumed to be familiar with Part 1 of this document.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Contents:

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 1 - Introduction

Key Principles

- A catalogue of security components has been defined that can be used to express security requirements for online services.
- For each component a set of levels has been defined with increasingly stringent requirements.
- The components and levels provide a language in which security requirements for online public services can be satisfied in order to claim compliance.

Security profiles should be constructed with the most appropriate levels. Levels may vary within each security case.

Status

1. This is a draft of the RSDOPS that is being made available for wider review and comment. It is being made available to all who have an interest on the understanding that it is still under review does not imply a commitment to release it as a formal standard. It should not be cited as part of a contractual agreement though its use is encouraged for informal discussions.

Security Components

2. This part describes a set of security components that can be used to express security requirements for online services. The components defined are not intended to be independent of one another. There is some overlap between components.

3. The degree of attention given to security within each component is captured in a set of levels, where Level 0 generally represents 'no specific security requirements' and the higher levels represent increasingly stringent requirements. Level 0 should be read as 'no specific requirements are expressed in this policy' or 'not relevant to this application'. It should not be read as 'no attention is needed to this component'.

4. For each level a set of requirements is defined that should be satisfied in order to claim compliance with the level. Examples showing where each level may be applicable are provided. Illustrations of how the requirements may be satisfied are also provided. The illustrative provisions do not represent the only way in which the requirements can be satisfied. They are not intended to constrain the possible solutions that service designers may adopt

5. The level numbering has no absolute significance and different components quote different numbers of levels. The security profile chosen for a particular

service should select levels most appropriate to that service and not necessarily choose the same numeric level for each component. The aim should be to build a comprehensive security case whilst avoiding over investment or excessive caution that might constrain the delivered solutions.

6. It should be noted that it is not intended for the components and levels to be a complete description of the security requirements for a service. There may be additional requirements that are specific to a particular service that are not covered by any of the components defined. In these circumstances these additional requirements will need to be documented as part of Step 5 of the requirements elicitation process in Requirement for the Secure Delivery of Online Public Services (RSDOPS) part 1 (Ref [b]) and documented in the security case.

Structure

7. The remainder of this Part of the document is organised as follows:

   a. Chapter 2 End user security components – this chapter covers the security components relevant to the people and businesses accessing the service;

   b. Chapter 3 Server security components – this chapter covers the security components relevant to the ICT hosting the service;

   c. Chapter 4 Network security components – this chapter covers the components relevant to the network infrastructure which is used to access the services;

   d. Chapter 5 Business logic security components – this chapter covers the components relevant to the software application that implements the service;

   e. Chapter 6 Assurance security components – this chapter covers the components relevant to gaining confidence in the end-to-end security of the public sector services.

Chapter 2 - End User Security Components

Key Principles

- Covers people and how they interact through the ICT used with the online public service.
- End users may access online public services for a variety of work related or non-work related reasons.
- The end user security components defined are:
    - Registration - the act of establishing the identity of a subject as a condition for obtaining a credential that can be subsequently used to reaffirm an identity. This may be personal registration in which the identity of a user is established or corporate registration in which the identity of an organisation and the user representing the organisation is established as well as the authority of the user to represent the organisation.
    - Authorisation - the process for establishing that a user is entitled to access a service.
    - Authentication - the process used to grant a user access to a service.
    - Privacy - the requirement for the responsible handing of personal and commercially sensitive information by a service.

Introduction

8. End user security components are those concerning people and their relationship to the ICT. People may interact with the ICT to access services for themselves, or on their organisation's behalf. In most (but not all) cases it is necessary to establish the authority of those individuals to access the service and the extent of the access granted.

9. End users may be members of the public, businesses, public sector employees or employees of the service providers.

10. End user security is considered under the following headings:

    a. Personal registration;

    b. Corporate registration;

    c. Authorisation;

    d. Authentication;

    e. Privacy.

Personal registration

11. Personal Registration is the act of establishing the identity of a subject as a condition for obtaining a credential that can be presented subsequently to obtain access to a service.

12. The requirements for confirming authority to access a specific service are described in the Authorisation requirements. Characteristics of the credentials themselves and their handling form part of the Authentication requirements.

13. The organisational, personnel and physical security requirements of the organisations providing the personal registration service are described in the Assurance requirements.

14. Four personal registration levels are defined that represent increasing levels of confidence that the social identity of the registrant has been correctly established.

15. In general, it is acceptable for a credential issued in support of a high registration level to be used to support a service requirement that may only require a lower level of registration. Privacy considerations will, however, need to be considered as higher levels of registration may unnecessarily expose more of the user identity details than need be.

Level 0 Personal registration – Not Required

16. Level 0 personal registration is appropriate in circumstances where the social identity (whether real or a pseudonym) of the user is not relevant to the service offered.

17. Services for individuals with no authentication requirements will, by implication, expect Level 0 User Registration. It should be noted that the service may still need to authenticate itself to the user.

Requirements

18. At Level 0 there are no service specific requirements for personal registration.

Examples

19. Level 0 personal registration is typically applicable to information-only services where nothing is known, or expected to be known, about the users. For example, a departmental website offering public information to individuals and businesses might call for Level 0 registration if the facility to tailor the site to the user's preference is offered.

Provision

20. Level 0 personal registration is likely to be provided using commercially based systems that have no national security certification using standard features of the product. Registration will typically be optional to access the service and might involve setting cookies to store user personalisation requirements. No private information needs to be stored by the service.

Level 1 Personal registration – Asserted

21. Level 1 personal registration is appropriate in circumstances where users, in order to gain access to a service, present an asserted identity which may imply a real-world identity but need not necessarily do so.

22. The nature of the credential will depend on the strength of authentication required. The distinguishing factor for a Level 1 personal registration service is that disclosure of the real identity of the user is not essential and a pseudonym may be offered.

23. Information provided to users through a service requiring only Level 1 registration may attract higher requirements for authentication, privacy and confidentiality. If Level 1 personal registration is associated with a higher level authentication requirement, care should be taken that the intent of the strong authentication is not undermined by lesser requirements for registration.

Requirements

24. The user is required to register before access to services can be granted. The user does not however need to disclose his or her real identity at registration.

25. The registration service should authenticate itself to the user. The strength of the authentication required will be dependent upon the registration information collected.

26. The registration service should make the user aware of any information and credentials that are to be stored on the user's machine and how to manage that information. The service should be designed to minimise risk to information transferred to the user's environment.

27. The registration information should be protected in transit between the user and the registration service where this information exchange occurs outside a trusted environment (see the Network Level Security Components for guidance on the level of protection).

28. Users should supply, or be issued with, unique access IDs and credentials. Access IDs and credentials do not, and might not claim to, represent any actual identity. An appropriately secure process should be used for the issuance of the credential.

29. Users should be made aware that they do not need to disclose a real identity and that they may offer a pseudonym.

30. Any self evident or inferred link to a real identity has no significance and should not be exploited by the service.

31. Where a user provides an electronic contact point (e.g. an email address), confirmation that the user is in control of that contact point should be obtained.

32. A suitably secure process should exist for the issue of registration credentials. These credentials should be protected while in transit and mechanisms should be in place to prevent their unauthorised use.

33. Users should be made aware of the legitimate uses of registration credentials. The registration credentials should indicate any limitations on their permitted usage.

34. A secure process should be in place to enable and encourage the timely reporting of suspected compromise of a credential.

35. Secure processes should exist that enable a user to maintain their registration information in response to changes in their circumstances.

36. Secure processes should exist that enable recovery from compromise or misappropriation of a registration credential.

37. Registration or revisions to registration information should be treated as accountable events. Accounting logs and audit information should be retained.

Examples

38. Level 1 personal registration is applicable to services where the user needs to create an account to build up, and return to, stored information but no association with a real identity is needed, or offered.

39. Level 1 personal registration may be associated with differing levels of authentication. A strictly pseudonymous service, for example a health check, may need strong authentication that matches the importance and sensitivity of the information.

40. Services which are primarily a purchase such as licensing may only need Level 1 personal registration as the identity of the applicant is not, strictly, an issue providing that payment can be completed. In the absence of anonymous electronic cash services, payment processing will, of necessity, expose a relationship with a real identity but this is an issue for registration for the payment service, not registration for the public sector service. For example, the

payment service may independently verify the identity of the user and authorise payment without revealing that identity to the service.

Provision

41. Level 1 registration will typically be performed wholly online. SSL/TLS will typically be used to secure communications between the registration authority and the registrant. Extended Validation Certificates may be needed by the Service Provider, dependent upon the nature of the information to be collected by the service. Information will be provided to the user on how to verify identity from the server certificate.

42. As part of the service registration process, a unique identifier is created that is associated with a credential. The type of credential required will be dependent upon the level of authentication the service requires.

43. If payment services are called up as part of the service, then the requirements of the payment service itself must be honoured.

Level 2 Personal registration – Tested

44. Level 2 personal registration is appropriate in circumstances where the service needs to collect and collate information on real individuals and pseudonymous registration is not appropriate.

45. Level 2 personal registration is primarily applicable to circumstances where registration will be conducted on-line and the immediate presence of the subject cannot be assumed. Potential users will need to present evidence that supports their identity claim, but the requirement for a traceable linkage to a real identity is not strong enough to merit rigorous independent face-to-face review and testing of the evidence. The testing of the evidence presented is expected to be sufficient for it to be offered in support of civil proceedings.

Requirements

46. Level 2 personal registration requires the user to present evidence of real identity as part of registration process.

47. The registration service should authenticate itself to the user at the start of the registration process. The strength of the authentication required will depend upon the registration information collected and should be in line with business need.

48. The registration service should make the user aware of any information and credentials that are to be stored on the user's client machine and how to manage this information. The risks associated with using unsecured or public access devices should be clearly articulated. The service should be designed to minimise these risks.

49. Users should be informed before the point of identity registration of:

    a. the use to be made of the identity registration information they submit and of any registration checks to be performed;

    b. their obligations and responsibilities to the service.

50. The registration information should be protected in transit between the user and the registration service where this information exchange occurs outside a trusted environment (see the Network Level Security Components for guidance on the level of protection).

51. Evidence offered should be tested using an assured process for strength and validity so that, on the balance of probabilities, the claim of the user is shown to be true. The presented evidence should be testable in order to establish to a reasonable level of confidence that the:

    a. claimed identity exists;

    b. registrant is the claimed identity.

52. Evidence that demonstrates that the claimed identity exists should establish the identity uniquely and should reference independently verifiable registers of identity such as birth certificates, passports, driving licences, electoral roll, NI Register, NHS register, Divorce Register, and employment records. This information may have been aggregated into a consolidated register. Negative information sources such as databases on deceased persons should also be consulted as part of the verification process.

53. Evidence that the registrant is actually the claimed identity should be tested through a challenge/response mechanism. This may involve the use of pre existing shared secrets. Alternatively a trusted independent channel to that individual (such as mailing registration codes to the verified address) may be used.

54. If the registrant offers an electronic contact point (such as an Email address), then user control of that contact point should be demonstrated before the system can use it.

55. Credentials issued to applicants must be issued in a secure manner. Users should be required to safeguard these credentials and not to share the credential with others.

56. Credentials should be protected while in transit and mechanisms should be in place to prevent their unauthorised use.

57. Users should be made aware of the legitimate uses of the registration credentials and any limitations on their use.

58. A secure process should be in place to enable and encourage the timely reporting of suspected compromise of a credential.

59. Users should be made aware of the processes to be followed to update their registration information or to cancel their registration when no longer required or when compromise of the registration credential may have occurred.

60. Secure processes should be in place to enable registration information to be maintained to reflect any changes in the user's circumstances. Evidence should be presented to authorise significant changes in information (such as external contact data) and this should be subject to the same level of testing as the initially provided information.

61. Processes that revoke a credential when required should exist. Such processes should ensure that any relying parties can determine whether the credential has been withdrawn.

62. Processes that permit identity repair in the event of identity compromise should exist.

63. Registration and changes to registration information should be treated as accountable events. Records should be maintained to enable retrospective independent review and validation of the evidence presented.

Examples

64. Level 2 personal registration is primarily applicable to those services where the service has a personal casework element and is to be delivered to a real individual entitled to receive the service, but where the nature of the service is such that the motivation for adversaries to misrepresent themselves as others, or registered users to misuse the service, is limited.

65. Services that are candidates for Level 2 personal registration include those where the value transfer is primarily from the individual to public body, such as tax collection, and there is limited opportunity for fraud through the creation of false identities.

66. Level 2 personal registration may also be applicable to some services, such as licence issue, where the value or benefit flows out from the public body to the individual if the benefit is traceable and can be subsequently withdrawn or the transaction reversed.

Provision

67. Provision of the basic electronic registration service will match that for Level 1 personal registration and the same implementation quality requirements will apply.

68. The discriminating factor for Level 2 personal registration is the provision of evidence that can bind the claimed identity of the registrant to a real identity without the need for face to face verification and the subsequent testing of that evidence.

69. As yet there is no reliable unique personal identifier. Typically first name, last name, date of birth, gender, nationality and current address are used to uniquely identify an individual and electronic verification services are used to verify the existence of an identity.

70. Prior to the introduction of any such service, other electronic verification service providers could be used. If such a service provider is used, the provider should:

    a. be registered with the Information Commissioner's Office as permitted to store personal data;

    b. have access to multiple, independent sources of identity information, not just electoral roll information;

    c. be able to link an applicant to both current and previous circumstances using a range of positive information sources;

    d. have access to negative information sources, such as databases on identity fraud and deceased persons;

    e. have transparent processes providing details of the checks that are carried out, the results of the checks, and how much certainty they give on the identity of the subject;

    f. allow the registration organisation to capture and store the information used to verify an identity.

71. Verifying a person’s claimed identity is more difficult. The preferred approach is through the use of pre existing shared knowledge. Selection of shared knowledge needs however to be made with care to ensure that the likelihood of an impostor also knowing the information is low. Other mechanisms that have been used include sending a onetime code to a known location of the claimed identity when the mailing delays can be tolerated. Risks associated with this should however be considered (e.g. shared post boxes in some residential properties) and appropriate measures put in place to manage them. Other routes can be used, such as telephone, but only if the telephone number can be

independently confirmed as belonging to the claimed identity and sufficient confidence exists that the risks associated with this route can be successfully managed.

72. Other established electronic identities may be available to vouch for the claimed identity of the registrant and may be offered in some cases. Care should be taken to ensure that the chain of evidence is properly traceable to a strong enough foundation identity and that single points of vulnerability are not unwittingly created.

Level 3 Personal registration – Verified

73. Level 3 personal registration is appropriate in circumstances where the service should be delivered to specific identified individuals and the nature of the service delivered is such that there is a significant risk that those individuals may seek to undermine the service, or that the service benefits may be diverted to those not entitled to receive them by impersonating entitled subjects.

74. The subject claims a real identity and the claimed identity is subject to rigorous testing to independently verify the claims. This testing includes rigorous review of the evidence and the demonstrable presence of the registrant. The process establishes the identity of the individual beyond reasonable doubt.

75. The testing of the evidence presented is expected to be sufficient for it to be offered in support of criminal proceedings or sanction. (This should not be taken to imply a requirement for evidential strength systems.)

Requirements

76. Level 3 personal registration requires the user to present evidence of identity as part of the registration process. The evidence offered should, as part of the process, be subject to rigorous testing that demonstrates beyond reasonable doubt that the identity claimed by the user exists and that the subject is the claimed identity and present at registration.

77. The registration service should authenticate itself to the subject at the start of the registration process. The strength of the authentication required will depend upon the registration information collected and should be consistent with business need.

78. The registration information should be protected where this information exchange occurs outside a trusted environment.

79. The subject should be informed before the point of identity registration of the use to be made of the registration information collected and of the types of checks to be performed to verify their identity. The consequences of providing fraudulent information should be explained.

80. The presented evidence should be testable in order to establish beyond reasonable doubt that the:

    a. claimed identity exists and is current;

    b. registrant is the claimed identity;

    c. the registrant is present and a willing subject at the registration.

81. The evidence presented should enable the unique identification of an individual. Any sensitivities associated with this (e.g. transgender, witness protection) must be considered and appropriate measures put in place to provide adequate security protection. The biographic footprint of the identity should be checked. The identity should be confirmed to be current including confirming no evidence of death/cessation of the identity, social interactions of the identity should be checked, and evidence that identity has been active should be sought. Any biographic and biometric information should be tested for duplicates.

82. Evidence that the applicant owns the identity might include third party corroboration of the claimant's identity from a trusted source, the use of shared pre existing secret knowledge, the applicant demonstrating possession of verified documents, and verification of a pre existing biometric against the applicant.

83. The applicant should be seen to be an active participant in, and present at, the registration and not apparently acting under duress or otherwise acting under the control of an adversary.

84. It should be confirmed that the registrant is unique and has not previously registered (unless there is a valid reason for multiple registrations). This should include checking the biometric and biographic data to confirm they are unique to the current applicant. Multiple registrations may be necessary to support for example transgender, witness protection, etc. Any sensitivities associated with an individual having been allowed to register multiple times should be explicitly considered and appropriate measures put in place to protect the existence of aliases.

85. Processes should be in place to enable registration information to be maintained to reflect any changes in the user's circumstances. Registrants should be able to review and update their information when required. The process for performing this should be subject to the same level of assurance as the initial registration.

86. The registrant should be informed of the processes to be followed in the event of changes in their circumstances or following an incident such as loss or other compromise of a credential.

87. A secure process should exist for the issue of registration credentials. These credentials should be protected while in transit and mechanisms should be in place to prevent their use by non registrants (e.g. PINs, biometrics, etc).

88. Users should be made aware of the legitimate uses of the registration credentials and any limitations on their use.

89. A secure process should be in place to enable and encourage the timely reporting of suspected compromise of a credential.

90. Processes should exist to enable a credential to be revoked when required. Such a process should ensure that any relying parties are made aware of the fact the credential has been revoked.

91. Processes should exist for identity repair in the event of identity compromise.

92. Registration and changes to registration information should be treated as accountable events. Records should be maintained to enable retrospective independent review and validation of the evidence presented.

93. Consideration should be given to the possibility that Level 3 personal registration data may be used as supporting evidence in bringing a case against the (alleged) user to seek redress for misuse of the service. If this is a possibility, then care should be taken that a proper chain of evidence is available and that record keeping and accounting is strong enough to support the case.

94. Credentials should be issued, and any biometric capture carried out, at the same time as identity validation to ensure that the same individual is registered on the system.

95. Users should be required to safeguard the credentials issued to them and not to share the credential with others.

Examples

96. Services requiring Level 3 personal registration are primarily those where there is significant benefit available to an adversary impersonating a legitimate subject, or the enrolled subject himself is a potential source of threat. It is appropriate where a user cannot be readily traced or a transaction reversed.

97. Example services include border controls and other physical access control. Financial benefit payments where the payments cannot be easily traced and recalled provide another example.

98. Services that attract a high level of personal accountability are likely to be candidates for Level 3 personal registration particularly where legal action may

be taken against potential adversaries and evidence is needed that implicates the individuals concerned.

99. It is likely that Level 3 personal registration will be associated with a requirement for the highest authorisation and authentication levels. It may be acceptable to use Level 3 personal registration data in support of lower authorisation and authentication requirements though doing so may compromise privacy at the lower levels.

Provision

100. Provision of Level 3 personal registration services takes place largely outside the ICT. Verification and validation of the individual and their entitlements is an administrative process that involves review of independent sources of identity information to confirm that the identity exists, review of documentary evidence presented by the registrant and interview of the registrants to confirm that they are the claimed identity.

101. As yet there is no reliable unique personal identifier. Typically first name, last name, date of birth, gender, nationality and current address are used to uniquely identify an individual and electronic verification services are used to confirm the existence of an identity. These are used to check the biographical footprint of the identity, to establish the relationship with their parents or guardians, check there are social interactions, that there is no evidence of death or cessation of the identity and that it has recently been active.

102. A national identity assurance service that can be used across government might be provided in due course. If available this would offer the preferred approach to verifying an identity. Prior to the introduction of any such service, other electronic verification service providers could be used. If such a service provider were used, the provider should:

    a. be registered with the Information Commissioner's Office as permitted to store personal data;

    b. have access to multiple, independent sources of identity information – e.g. not just electoral roll information;

    c. be able to link an applicant to both current and previous circumstances using a range of positive information sources;

    d. have access to negative information sources, such as databases on identity fraud and deceased persons;

    e. have transparent processes providing details of the checks that are carried out, the results of the checks, and how much certainty they give on the identity of the subject;

f. allow the registration organisation to capture and store the information used to verify an identity.

103. Verifying a person's claimed identity is more difficult. The preferred approach is through the use of shared knowledge. Selection of pre-existing shared secret needs however to be made with care to ensure that the likelihood of an impostor knowing such information is low. Other checks that can be performed include obtaining third party confirmation of the identity, requiring the registrant to be in possession of valid documents, through the applicant's knowledge of the personal history of the identity and through the matching of existing biometrics.

104. Documentary evidence that can support the validation of an identity includes, for example a:

a. current passport;

b. current full UK driving licence (including photocard);

c. current UK provisional photocard driving licence; or

d. current Armed Forces Identity Card.

105. Evidence of current address might include, for example:

a. a current full UK driving licence (if not already used as evidence of identity);

b. a current UK provisional photocard driving licence (if not already used as evidence of identity);

c. a recent bank, building society or credit union statement or passbook (with printed address);

d. a recent utility bill (such as gas or electricity, not a mobile phone bill);

e. a recent Local Authority tax bill,

f. recent original mortgage statement;

g. a recent benefits book or Benefits, Agency/Department for Work and Pensions Notification letter;

h. Solicitor's correspondence (relating to a house purchase and less than 2 months old);

i. a recent Local Authority rent card or Local Authority tenancy agreement.

106. Documentary evidence should be originals or certified copies. A risk based approach is likely to be followed in verifying the identity of an applicant. The use of statements printed from the Internet is not acceptable.

107. It is likely that Level 3 personal registration will take place in specific facilities designated, and designed, for that purpose and will include a face to face interview with the applicant and collection of biometrics.

108. Owing to the need for demonstrable presence of the registrant, remote personal registration at Level 3 is currently not envisaged though tools and techniques to achieve this might be the subject of future development.

Corporate registration[1]

109. Corporate registration is the process of establishing the:

    a. identity of an organisation;

    b. identity of the individual registering the organisation;

    c. authority of the individual to undertake the registration on behalf of the organisation.

110. The requirements for confirming authority to access a particular service are described in the Authorisation requirements. Technical characteristics of the credentials themselves and their handling form part of the Authentication requirements. The organisational, personnel and physical security requirements of the organisations providing the corporate registration service are described in the Assurance requirements.

111. Three corporate registration levels are identified that represent increasing levels of confidence that the identity and authority of the registrant has been correctly established.

112. In general, it is acceptable for an identity credential issued in support of a high registration level to be used to support a service requirement that may only require a lower level of registration. The converse is likely to be unacceptable.

Level 0 Corporate registration – Not Required

113. As with Level 0 Personal registration, Level 0 corporate registration is appropriate where the identity of the organisation has no significance to the service offered.

---

[1] The registration process relevant to a sole trader is personal registration, rather than corporate registration.

114. Services for organisations with no authentication requirements will by implication have a Level 0 corporate registration requirement.

Requirements

115. At Level 0 there are no service specific requirements for corporate registration.

Examples

116. Level 0 corporate registration is typically applicable to information only services where nothing is known, or expected to be known, about the users.

Provision

117. Level 0 corporate registration is intended to apply to commercially based systems that have no national security certification and where standard features of the product are used. Registration will typically be an option to access the service and might involve setting cookies to store user personalisation requirements. No private information will be stored by the service.

Level 1 Corporate registration – Asserted

118. As with Level 1 personal registration, Level 1 corporate registration is appropriate in circumstances where users are required to register to access the service but do not need to disclose their personal identity or that of their organisation.

119. In order to gain access to the system, users will present a chosen identity (which may be a pseudonym) and a credential that will be used when gaining access to the service. The nature of the credential will relate to the strength of authentication required. The distinguishing factor for a Level 1 corporate registration service is that the real identity of the user or the organisation they are representing is not required and inferences about the real identity may not be exploited.

120. Any commercially sensitive information solicited is not linked to or shared with external bodies. Real identification information is not necessary to obtain authorisation to use the service. Information provided by the user may still need to be safeguarded. It is noted that information provided by registrants through a service requiring only Level 1 corporate registration may attract high requirements for authentication, privacy and confidentiality.

121. If Level 1 corporate registration is associated with a higher level of authentication requirement, care should be taken that the intent of the strong authentication is not undermined by the lesser requirements for registration.

Requirements

122. The user should register before being granted access to the service. The user is not required to expose his or her actual identity or the organisation that they represent.

123. The registration service should authenticate itself to the user by the start of the registration process. The strength of the authentication required will depend upon the registration information collected and should be in line with commercial good practice.

124. The registration service should make the user aware of any information and credentials that are to be stored on the user's client machine and how to manage this information. The service should be designed to minimise the risks associated with the storage of sensitive information on the client's machine.

125. The registration information should be protected in transit between the user and the registration service where this information exchange occurs outside a trusted environment (see the Network Level Security Component for guidance on the required level of protection).

126. Users should supply, or be issued with, unique access IDs and credentials. Access IDs and credentials need not, and may not claim to, represent any actual identity. A secure process must be used to issue any credentials.

127. Where a user provides an electronic contact point (e.g. e-mail address), confirmation that the registrant is in control of that contact point should be obtained.

128. Secure processes should exist that enable a user to maintain their registration information to account for changes in their circumstances.

129. Secure process should exist for the issue of registration credentials. These credentials should be protected while in transit and mechanisms should be in place to prevent their unauthorised use.

130. Users should be made aware of the legitimate uses of the registration credentials and any limitations on their use.

131. A secure process should be in place to enable and encourage the timely reporting of suspected compromise of a credential.

132. Secure processes should exist that enable compromise or misappropriation of a registration credential to be handled.

133. Registration or revisions to registration information should be treated as accountable events. Accounting logs and audit information should be retained.

Examples

134. Level 1 corporate registration is applicable to services where the user is required to create an account to build up, and return to, stored information but no connection is needed, or offered, to a real identity. For example, completion of a licence application that is subsequently printed, signed and posted to the relevant organisation.

135. Services which are primarily a purchase for which payment provides sufficient authority for access are typical of services requiring Level 1 registration (e.g. download of documents from Companies Houses, Land registry documents, chart information available from UK Hydrographic Office). Payment processing will, of necessity, imply a linkage to a real identity but this is an issue for registration for the payment service, not registration for the public sector service.

Provision

136. Level 1 registration will typically be performed online. TLS with Enhanced Validation Certificate and with information being provided to the user on how to verify identity from the server certificate will typically be used to verify the identity of the registration service. As part of the service authorisation process a unique identifier is created that is associated with a credential. The type of credential required will be dependent upon the level of authentication the service requires.

137. If payment services are called up as part of the service, then the requirements of the payment service itself should be honoured.

Level 2 Corporate registration – Tested

138. Level 2 corporate registration is appropriate in circumstances where the service collects and collates information related to real organisations and pseudonymous registration is not appropriate.

139. Potential users will need to present evidence that supports their real identity, the identity of the organisation they represent and that they are authorised to perform the registration on behalf of that organisation.

140. The requirement for a traceable linkage to identity is, however, not strong enough to merit rigorous independent face-to-face review and testing of the evidence. It may however be cited in support of a civil prosecution.

141. Level 2 corporate registration is primarily applicable to services where registration should be conducted remotely and there is limited opportunity to test the validity and quality of the information presented.

Requirements

142. Level 2 corporate registration requires the user to present evidence of organisational identity, their identity and their authority to register on behalf of the organisation as part of registration for access to the service. Evidence offered should be tested for strength and validity so that, on the balance of probabilities, the claims of the registrant are shown to be true. Evidence of their identity should be verified in accordance with either level 2 or level 3 personal registration.

143. The registration service should authenticate itself to the user. The strength of the authentication required will depend upon the registration information collected and should be in line with business need.

144. The registration service should make the user aware of any information and credentials that are to be stored on the user's client machine and how to manage this information. The service should be designed to minimise the risks associated with this.

145. Registrants should be informed at or before the point of identity registration of the intended use to be made of the identity registration information they submit and of any registration checks to be performed. The registrant should be informed of the penalty for fraudulent application.

146. The registration information should be protected in transit between the user and the registration service where this information exchange occurs outside a trusted environment (see the Network Level Security Components for guidance on the required level of protection).

147. The evidence offered should be tested using an assured process for strength and validity so that, on the balance of probabilities, the claim of the user is shown to be true. The presented evidence should be testable in order to establish to a reasonable level of confidence that the:

    a. claimed organisation exists;

    b. claimed user identity exists;

    c. registrant is the claimed user;

    d. user has the authority to register on behalf of the organisation.

148. The identity of an organisation is the set of attributes that together uniquely identify the organisation. Within the UK there is no single official or statutory attribute or set of attributes that is used to uniquely identify organisations, nor is there an official or statutory document or other credential to demonstrate that identity. Most organisations will have a set of attributes, some or all of which

uniquely identify them to a wide range of parties, including government. As a minimum these attributes will include the name by which an organisation is known and the address at which it undertakes its principal activities.

149. Evidence that demonstrates that the claimed organisational identity exists should establish the identity uniquely and should reference independently verifiable registers. Negative information sources such as databases of dissolved companies or databases on identity fraud should be consulted as part of the verification process. The biography of the identity should be checked. Evidence of recent trading should be obtained.

150. The evidence that the claimed identity of the user exists should satisfy the requirements of Level 2 or Level 3 personal registration. The level required will be dependent on business need.

151. Evidence that the registrant is actually the claimed identity and has the authority to register on behalf of the organisation should be tested through a challenge/response mechanism that can validate a trusted independent channel to a known official of the organisation concerned.

152. A secure process must be used to issue the registration credentials. Secure process should exist for the issue of registration credentials. These credentials should be protected while in transit and mechanisms should be in place to prevent their unauthorised use.

153. Users should be made aware of the legitimate uses of the registration credentials. The registration credentials should contain information on any limitations on their use.

154. A secure process should be in place to enable and encourage the timely reporting of suspected compromise of a credential.

155. Processes should be in place to enable registration information to be maintained and reflect any changes in the user's and organisation's circumstances. Registrants should be able to review and update their information when required. The update process should be subject to the same level of testing as initial registration.

156. The organisation registering should be required to inform the registration authority in the case of any substantive change in circumstances, including cases where an issued credential should be revoked.

157. Effective processes to revoke a credential when required should exist. Such processes should ensure that any relying parties are aware of the fact that the credential has been withdrawn.

158. Processes that enable identity repair in the event of compromise should exist.

159. Registration and changes to registration information should be treated as accountable events. Records should be maintained to enable retrospective independent review and validation of the evidence presented.

Examples

160. Level 2 corporate registration is primarily applicable to those services where the service is delivered to a real organisation entitled to receive the service, but where the nature of the service is such that the motivation for adversaries to misrepresent themselves as others, or registered users to misuse the service, is limited.

161. Services that are candidates for Level 2 corporate registration include those where the value transfer is primarily from the business to government, such as making PAYE or NIC, VAT and corporation tax collection, and there is limited opportunity for fraud through the creation of false identities.

162. Level 2 corporate registration may also be applicable to some services, such as e-procurement, where the value or benefit flows out from government to the business if the benefit is traceable and can be subsequently withdrawn.

Provision

163. Provision of the basic electronic registration service will match that for Level 1 corporate registration and the same implementation quality requirements will apply.

164. The discriminating factor for Level 2 corporate registration is the provision of evidence that can bind the claimed identity to a real identity without the need for face to face or site visit verification.

165. As yet there is no single unique identifier for all organisations. Corporate organisations have certain legally required attributes, which can be regarded as defining identity. These includes its:

    a. registered number;

    b. registered corporate name and any trading names used;

    c. registered address and any separate principal trading addresses.

166. Certain other organisations also register with official statutory or other governing bodies (e.g. Charities, Solicitors, and Accountants). In this case, it will be the attributes by which they are known and recognised to such bodies that will be required to be validated during registration. One particular attribute, which often

acts as a de facto “official” registration for most trading bodies, is the VAT registration number.

167. Where a public registration is required for an organisation (e.g. Limited Liability Partnership, Limited or Public Limited Company, Charity) the relevant official registration authority is consulted (e.g. Companies House, Charity Commissioners) to validate the organisational identity. In other cases a commercial organisation providing acceptable identity services may need to be used.

168. As with Level 2 personal registration, an electronic identity service provider should:

    a. be able to link an applicant to both current and previous circumstances using a range of positive information sources;

    b. have access to negative information sources, such as databases on identity fraud, closed companies, etc.;

    c. have transparent processes providing details of the checks that are carried out, the results of the checks, and how much certainty they give on the identity of the subject;

    d. allow the capture and storage of the information used to verify an identity.

169. Provision of personal identification service for the registrant’s representative is the same as for Level 2 or Level 3 personal registration.

170. Confirmation that the user is the claimed identity and has the authority to perform the registration is more difficult. It may involve the use of shared secrets. Selection of shared secrets needs however to be made with care to ensure that the likelihood of an unauthorised person knowing the information is low. Other mechanisms include sending a onetime password to a known official of the organisation at a known address where the mailing delays can be tolerated. Risks associated with this should however be considered and appropriate measures put in place to manage them. Other routes can be used, such as telephone, but only if the telephone number can be independently verified as belonging to the claimed identity and the name of an appropriate official to contact is known. Again the risks associated with this approach should be carefully considered and appropriately managed.

171. Other established electronic identities may be available to vouch for the claimed identity of the registrant and may be offered in some cases. Care should be taken to ensure that the chain of evidence is properly traceable to a strong enough foundation identity and that a single point of vulnerability is not unwittingly created.

Authorisation

172. Authorisation is the process by which a registered user's entitlement to access a particular service is confirmed and authorisation is then granted to access the service for a defined period. It includes validation of some attributes of a subject to enable their entitlement to access a service to be validated. The attributes that will require validation will be service specific as will the level of validation required. Authorisation also covers the circumstances in which a person or company acts as a proxy or agent. Their authority to do so needs to be verified.

173. It covers the processes required to:

    a. establish the validity of any attributes of a potential service user;

    b. confirmation that the validated attributes entitle the potential user to access the service;

    c. the provision of any service specific credentials/account to enable that access;

    d. suspend, revoke or disable a credential/account as required.

174. The attributes that need to be presented and validated to confirm entitlement to access a particular service will be service specific.

175. The organisational, personnel and physical security requirements of the organisations providing the Authorisation service are described in the Assurance requirements.

176. The technical characteristics of the credential themselves and their handling form part of the Authentication requirements.

177. This section defines two Authorisation levels that represent increasing levels of validation of the attributes of a user. They involve obtaining increasing levels of confidence that a user is entitled to use the service.

178. For services that require checks to be performed on a claimed real identity for access to be provided, authorisation may be performed at the same time as registration. There is, however, often a preference for authorisation to be delayed until first use of the service is required by the user. If authorisation is performed after registration, the identity credential issued as part of the registration process will need to be used to support the authorisation either directly or indirectly.

179. Although registration initially establishes identity, the process of verifying an identity is a cumulative process. Authorisation for a particular service may offer the opportunity to gain additional assurance on the identity of the individual

through a shared secret or for changes in circumstances of a user since registration to be identified. Full advantage of these opportunities should be taken. It should be noted that not all services will need or offer this opportunity.

180. For some business services, it may be necessary to look beyond the identity of the user to determine the controlling interest or the identity of the individuals owning or running the organisation represented by the users. Where required this should be done as part of service authorisation.

Level 0 Authorisation – Implicit

181. At Level 0 there is no explicit requirement to verify the entitlement of a user to access the service.

Requirements

182. There are no service specific requirements for authorisation.

Examples

183. Level 0 authorisation is typically applicable to information only services where nothing is known, or expected to be known, about the users. Visibility of the service is considered to be authority to use it.

Provision

184. Not applicable at this level – Authorisation by virtue of service visibility may be inferred from a prior network authentication.

Level 1 Authorisation – Tested

185. At level 1 the entitlement of the user to access the service is tested. This may be based on evidence offered by the user themselves or, once the service has established the identity of the registrant, evidence of entitlement may be tested within the service itself.

186. Level 1 authorisation may be associated with Level 1, Level 2 or Level 3 Personal Registration or Level 1 or 2 Corporate Registration.

Requirements

187. The authorisation service should authenticate itself to the user. The strength of the authentication required will depend upon the authorisation information to be collected, what the service authorisation is for, and should be appropriate to the business need.

188. The authorisation service should make the user aware of any information and credentials that are to be stored on the user's client machine and how to manage this information. The risks associated with using unsecured or public

access devices should be clearly articulated. The service should be designed to minimise these risks.

189. The authorisation service should make the user aware of any conditions of use for the service and obtain their agreement to these terms. The user should be informed of any changes in their circumstances that they should report to the service to enable their continued entitlement to use the service to be assessed. The user should be made aware of their obligations to keep any sensitive information secret and to securely store any issued credentials.

190. The authorisation service should make the user aware of any measures the user should take to protect any credential issued as part of the authorisation process and obtained their agreement to these terms. The user should be made aware of the exception-handling and incident reporting processes to be followed.

191. The authorisation evidence requested should be the minimum required in order to confirm a user's authorisation to use the service. Confirmation of entitlement should be based on the 'balance of probabilities'. Where necessary, 'Out of band' mechanisms may be required to confirm authority/entitlement. The status of any registration credentials used as part of the authorisation process should be checked to ensure they are valid.

192. Authorisation information should be protected in transit between the user and the authorisation service where this information exchange occurs outside a trusted environment (see the Network Level Security Components for guidance on the level of protection).

193. Credentials used to access the service should be issued in a secure manner. Where tokens are used, the passwords used to protect access should be delivered separately to the token. Users of the credentials should be required to protect the privacy of the password and not to share the credential with others.

194. Credentials issued should normally have limited life-span and should normally be subject to suspension following a set period of inactivity. The appropriate lifetime and the period of inactivity that results in suspension will be service dependent. In some cases it may be appropriate to establish normal usage patterns and disable credentials if there are significant deviations from these patterns.

195. A secure process should exist for the issue of registration credentials. These credentials should be protected while in transit and mechanisms should be in place to prevent their unauthorised use.

196. A secure process should be in place to enable and encourage the timely reporting of suspected compromise of a credential.

197. Secure processes should exist that enable a user to maintain their authorisation information and account for changes in their circumstances

198. Clear procedures should be in place to enable users to terminate authority to use a service and to revoke a credential.

199. Secure processes should be in place to enable a user to recover their authorisation credentials in the event of loss or damage.

200. Process should be in place to review the continued entitlement of users to be enrolled in a service and to suspend or remove users who are no longer entitled.

201. Authorisation or revisions to authorisation information should be treated as accountable events. Accounting logs and audit information should be recorded.

Examples

202. Services involving low value purchase provide examples of services for which Level 1 authorisation may be appropriate. Confirmation of payment will be sufficient evidence of entitlement to access the service. For other services presentation of the agreed credential and shared secret may provide sufficient evidence of entitlement.

203. Services that are candidates for Level 1 authorisation include those where the value transfer is primarily from the business to government, such as making PAYE or NIC, VAT and corporation tax collection, and there is limited opportunity for fraud through false authorisation.

204. Level 1 authorisation may also be applicable to some services, such as e-procurement, where the value or benefit flows out from government to the business if the benefit is traceable and can be subsequently withdrawn.

Provision

205. Level 1 authorisation will typically use standard commercial systems but will require additional testing to show that there are sufficient quality checks in place and that the system makes clear to the users the purpose and scope of authorisation.

206. For some services confirmation of entitlement will be based on confirmation of payment. The requirements of the payment service will need to be met in these circumstances.

207. For some services (e.g. some business services), the claimed authority of the user will need to be validated through out of band techniques (for example, by

contacting a known official of the organisation at a known address or telephone number to confirm the role of a user).

208. In all cases an appropriate chain of evidence will need to be maintained to allow independent validation of the decision to enrol a user.

Authentication

209. Authentication is the last step in the process by which an authorised service user is granted access to use a service.

210. This section defines four authentication levels that represent the degree of confidence that the electronic identity quoted during authentication matches the registered identity for that account.

Level 0 Authentication – Not Required

211. For a Level 0 service no explicit authentication actions are required to access the service but untested session context (such as cookies) might be set. Misappropriation of this session information will have no consequence.

Requirements

212. In simple cases, there are no requirements for user authentication. In restricted environments, there may be authentication requirements for access to the environment in which the service is offered (e.g. access to a corporate system), and these will be defined by the system used for access.

213. If session context information is set the user should be made aware of this.

214. Level 0 services should not retain information that allows the service user to be identified and should not retain details of payment instruments such as credit cards.

215. Depending on the type of service offered there may be a requirement for the public sector service to authenticate itself to the user. If this is the case commercial good practice should be followed.

216. Controls should be in place to prevent unauthorised users obtaining access to key system data including account identifiers and password files.

Examples

217. Level 0 Authentication services are typically information only services that require no information from or about the users. Most departmental public web sites will fit into this category as they are primarily offering freely downloadable information and documents.

218. Services that involve simple purchasing activities may be Level 0 if the service does not need to retain personal information about the subscriber and the requirements of any payment service are satisfied.

Provision

219. No user authentication service is required. Server authentication, when required is likely to involve the use of TLS with users being encouraged to explicitly confirm the provenance and validity of the server's certificate.

Level 1 Authentication – Minimal

220. Level 1 authentication is applicable to public sector services where user authorisation is mandated but strong anti-replay measures are not justifiable. The user will typically be required to expose an authentication secret that was agreed at authorisation.

Requirements

221. Level 1 authentication should not be used for services where private or commercially sensitive information will be collated and stored by the service that attracts a Privacy level of 1 or higher (see Para 289).

222. The service should authenticate itself to the user prior to starting the user authentication session. This should be done in accordance with business need and is expected to comply with commercial good practice.

223. The service should make the user aware of:

    a. any information and credentials that are to be stored on the user's client machine

    b. the risk associated with the use of unsecured or public access systems and, preferably, offers an access mode that leaves no persistent information on the client device.

224. Users should be informed of any special measures they need to take before, during, and after client sessions.

225. As part of the authentication process, the user should demonstrate possession of an authentication credential that was issued during the authorisation process. An authentication secret may be directly quoted during authentication. Authentication secrets should however be protected in transit across any untrusted networks (see the Network Level Security Components for guidance on the required level of protection).

226. Good password disciplines should be maintained, and the systems should be designed to enforce these disciplines. This includes processes for ensuring

password quality, password protection and for the password replacement after prolonged use (see for example CESG Information Assurance Memorandum 26, Ref [c]).

227. The system should be designed to minimise or eliminate internal exposure of passwords.

228. The system should be designed to minimise the threat from exhaustion, dictionary, or other automated attacks.

229. Controls should be in place to prevent unauthorised access to key system data including account identifiers and password files.

230. Users should be informed of the exception-handling procedures that are in place (such as suspected loss or compromise of a credential). These procedures should be easily accessible to the user.

231. A secure process should exist for user account recovery (e.g. in the event of a user forgetting his/her password). This should be at least as secure as the initial authorisation process.

232. Accounting logs and audit information should be recorded supported by appropriate monitoring and accounting procedures to enable potential attacks on the system to be detected and appropriate mitigation measures taken. A chain of evidence should be maintained to enable users to be held accountable for their actions (see Accountability and Situational Awareness security components).

Examples

233. Examples of transactions that might merit Level 1 authentication include:

    a. A client makes an application or initiates a transaction that will be completed on the basis of a paper form. The service that allows the user to create and populate an electronic facsimile of the paper form which will contain personal information that should be protected, but may only need Level 1 protection.

    b. A client participates in on-line training. There is a need for authentication such that the client is recognised by the service and connected to the appropriate place in the course or given relevant assignments and grades.

    c. On-line purchase of a service – where personal information is stored for the convenience of the user.

Provision

234. Level 1 authentication services will typically be implemented using username/password logins with system generated or user chosen passwords. Passwords will be subject to quality checks and technical measures, such as TLS access over HTTP, will be used to provide service authentication and to minimise the risk of password or other sensitive information capture in transit over the network.

235. At Level 1, replay protection is not required, static passwords are generally sufficient. On-line password resets are likely to involve demonstration of a subset of a set of shared secrets agreed during authorisation. The subset will be different for each reset request.

236. It is likely that good quality commercial password systems will suffice for Level 1.

Level 2 Authentication – Robust

237. At Level 2, the user is required to demonstrate possession of unique knowledge agreed at, or items issued at, registration without disclosing anything that could be captured by an observer and replayed to falsify a transaction.

238. The requirement may be met through use of a suitable token, or a challenge/response session that invites the user to demonstrate partial knowledge from a set of memorable information items where successive challenges invite the release of different subsets of the knowledge – often referred to as shared secrets.

239. At this level an assumption is made that the authorised user is generally cooperative and well intentioned.

Requirements

240. Measures should be in place to prevent and other impersonation attacks. Consideration of the prevention of man-in-the-middle attacks in both client to server and server to client communications will be required.

241. The service should authenticate itself to the user prior to starting the authentication session. This should be done in accordance with good commercial practice.

242. The service should make the user aware of:

    a. any information and credentials that are to be stored on the user's client machine;

b. the risk associated with the use of unsecured or public access systems and, preferably, offering an access mode that does not leave persistent information on the client machine.

243. Users should be informed of any special measures that they need to take before, during, and after client sessions.

244. If a memorable information system is used:

a. the knowledge space must be large enough for a chance replay attack to have a low probability of success without demanding too much of the user's ability to recall the knowledge;

b. good disciplines should be maintained in selecting the shared secrets, and the systems should be designed to enforce these disciplines [d]. It is essential that the envisaged attacker is considered in designing such systems (e.g. family members);

c. users should be able to change the memorable information as it become stales, incorrect, or possibly compromised;

d. the system should be designed to minimise or eliminate internal exposure of the shared secrets;

e. the system should be designed to minimise the threat from brute force, dictionary and other automated attacks;

f. provision should be made to enforce renewal of secrets after a elapsed period of time and after frequent use.

245. The memorable information approach should be considered as an interim measure pending the introduction of stronger two factor based schemes.

246. If tokens are used in support of Level 2 authentication they:

a. should be protected against duplication;

b. their status should be checked;

c. where theft of the token is possible, it should be ensured that the credential is only usable in conjunction with collateral information such as a password/PIN. Good password disciplines should be maintained (see for example CESG Information Assurance Memorandum 26 [c]).

247. Explicit consideration of when authentication is required should be given. For example, the need to authenticate both to access the service and on initiating significant transactions should be considered.

248. Users should be informed of the exception-handling procedures that are in place (such as reporting actual or suspected loss of a token). These procedures should be easily accessible to the user.

249. Accounting logs and audit information should be recorded and supported with appropriate monitoring and accounting procedures. Forensic examination of the use of the service should be possible to allow potential attacks to be detected and appropriate mitigation measures to be taken. Evidence relating to suspected errant user activity should be appropriately managed to ensure that it may be cited in support of civil recovery actions. Accounting and audit requirements are defined in more detail in the Accountability and Situational Awareness security components.

Examples

250. Level 2 authentication is appropriate for personal casework services where the customer is generally motivated to make successful use of the electronic service delivery option and the primary threat is misuse by unauthorised individuals. The majority of services that are delivered to specific individuals will require Level 2 authentication, this includes such services as tax and benefit accounts, pensions, and welfare.

Provision

251. There are several technical approaches that can provide the essential additional protections needed for Level 2 over that provided by Level 1. The simplest, and lowest implementation cost, is to use a memorable information approach where the service and the user agree memorable information such as pre placed questions or a password and, during authentication, ask a subset of the questions or for particular letters from the password using different random choices for each session. This approach has usability and security issues than make it less suitable for longer term use.

252. Tokens general provide a stronger solution providing they are protected against duplication. If unprotected tokens such as magnetic stripe cards that can be readily duplicated are to be used the risks associated with this will need to be considered. Tokens that can encrypt a onetime challenge, or a rolling time based counter, are preferable but may have significant logistical and cost implications.

253. Other technologies that might be suitable include sending a onetime password to the user by phone or text message. Consideration of the protection required for this password while in transit needs however to be carefully considered and there may be usability and diversity concerns that rule it out as a universal solution.

254. Technology continues to advance in this area and new products should be assessed for their suitability. Use of commercial technology will be subject to a proper review, and possible evaluation, of the security.

Level 3 Authentication – Accountable

255. At Level 3, service authentication is required to collect strong evidence that the individual requesting the service is actually the person registered, and is present at the time of authentication.

256. Level 3 authentication is also required to support mandatory authentication of potentially unwilling subjects who may be strongly motivated to take action to cause a failure to authenticate, or to be authenticated as a different enrolled subject who may or may not have been complicit in the attempt to falsify the authentication.

257. At Level 3 the authentication measures should resist unwilling or malicious authorised users, correctly categorise non-authorised subjects, and collect evidence that can hold malicious subjects to account for their actions.

Requirements

258. Strong measures should be in place to prevent man-in-the-middle and other impersonation attacks including strong authentication of the service to the user. Separate consideration should be given to communications from the client to the server and from the server to the client.

259. The client used to access the service should not be trusted to protect the credential unless the service is able to validate any assumptions made (e.g. the service provides secure kiosks to enable user access of the service).

260. Tokens used in support of Level 3 authentication should be protected against duplication. The token should only be usable in conjunction with collateral information such as a password/PIN. Good password discipline should be maintained (see for example CESG Information Assurance Memorandum 26 [c]).

261. Where threats from the user cannot be discounted the token must have tamper protection that is capable of resisting attack from a skilled attacker. Guidance on the appropriate measures should be sought from the National Technical Authority (CESG).

262. Users should be made aware of, and should agree to, the measures they should take to protect the token and the consequences of not following the measures.

263. Users should be informed of the exception-handling procedures that are in place (such as the suspected loss of a token) and agree to follow these procedures in a timely manner when required.

264. Accounting logs and audit information should be recorded supported by appropriate monitoring and accounting procedures to enable forensic examination of the use of the service and to allow potential attacks to be detected and appropriate mitigation measures to be taken. Consideration should be given to the possibility that audit information may be used as supporting evidence in bringing a case against the (alleged) user to seek redress for misuse of the service. If this is a possibility, then care should be taken that a proper chain of evidence is available, and record keeping and accounting is strong enough to support the case. Accounting and audit requirements are defined in more detail in the Accountability and Situational Awareness security components.

265. If Biometric Technology is used to support Level 3 authentication, the security properties that the biometric system should possess are that:

    a. there should be a low probability that an enrolled user will be incorrectly identified as a different enrolled user;

    b. there should be a low probability that a hostile user can bring about a deliberate failure to identify;

    c. the system should be resistant to the use of artefacts that could be employed to authenticate an enrolled user who is not present;

    d. the system should have a low probability that a subject will fail to enrol correctly, either through natural body characteristics, or deliberately caused.

    e. The system should be usable, acceptable to its target user base, and suitable for its intended application.

266. CESG Infosec Memorandum 28 [e] provides the detailed guidance that should be complied with.

267. Explicit consideration of when authentication is required should be given. For example, the need to authenticate both to access the service and on initiating significant transactions should be considered.

Examples

268. Level 3 authentication is applicable, for example, to border control and law enforcement applications where the physical movement of people, or non recoverable benefit transfer, is the issue. Biometric identity cards could be use

to support a number of government services including immigration controls, driver identification, and authorising medical treatment.

269. Remote (unsupervised) application of Level 3 authentication will be limited by the ability to adequately assure the binding of an offered credential to a real, and present individual.

Provision

270. Level 3 authentication may incorporate a degree of biometric technology to demonstrate the actual presence of the enrolled person. This is particularly relevant if the user is likely to be unwilling to verify their identity. Depending on the application, this may be configured as true authentication (substantiating a claimed identity), or identification (establishing the identity without a supporting claim). If biometric technology is to be used, reference should be made to the significant body of material that has been developed to assist in the choice and assessment of biometric technologies and products (see for example the guidance material available on the CESG website [f]).

271. Biometrics may not however be essential at Level 3 in circumstances where the authentication is needed primarily to support strong accountability but the threat arising from the user themselves can be discounted. In this case, a recognised signing device (e.g. Chip and Pin) may be sufficient to support the strong accountability at Level 3. Strong accounting requirements will however need to be associated with the token/signing devices.

Privacy

272. Privacy is a requirement for socially responsible handling of personal and commercially sensitive information. Individuals and businesses have a reasonable expectation that measures are in place to ensure that the information collected by a service:

    a. is the minimum necessary to fulfil its purpose;

    b. is only accessible to those with a legitimate need to know;

    c. is used only for the declared purposes for which it was collected;

    d. is maintained to ensure its continuing validity and quality;

    e. is disposed of in a secure manner when no longer required.

273. Assurance must be provided to the individual and the business that these expectations are being met and that information held on them can be presented to them on request.

Level 0 Privacy – No Statement

274. At Level 0 no private information is collected by the service.

Requirements

275. There are no specific Privacy requirements. A PIA [g] assessment may need to be performed to confirm this.

Examples

276. Examples of services likely to fall into this category include those:

    a. that provide information only services, for example, departmental websites offering free downloadable information which do not set cookies or devices that can be used to track the browsing history of a user.

Provision

277. Provision is likely to involve the use of standard features of commercially based systems. No particular Privacy Enhancing Technology need be utilised.

Level 1 Privacy – Implicit

278. At Level 1 the service is designed to minimise its privacy impact on prospective users. Privacy related objectives are considered alongside business goals, and privacy considerations are addressed at every stage of the service's lifecycle [h].

Requirements

279. The organisation providing the service should have an overall privacy policy/information charter. This policy defines the baseline privacy risk tolerance and appetite of the organisation. This document should be made available to the public.

280. An effective privacy management system should be in place to safeguard the private information collected. This includes an appointed executive level representative who can be held accountable for proper management of the private information.

281. Privacy requirements should be considered at the outset of the project to deliver the service. The private information to be held by the service should be explicitly identified. A privacy impact assessment (PIA) should be performed in accordance with ICO's guidance [g]. The assessment should consider all components of privacy from the perspective of the individual rather than the organisation. Compliance assessment with relevant legislation (e.g. Data Protection Act) should be performed.

282. The privacy risks identified should be effectively managed throughout the life of the service. The privacy risks will be one factor in determining the appropriate security levels for the different security components.

283. A privacy policy/privacy impact assessment for the service should be placed in the public domain so that potential users of the service have access to it. Some of the information within the PIA report may be subject to security or commercial sensitivities. In such cases, it may be appropriate for the detailed information to be in restricted access appendices.

284. The sharing of the private information within the organisation and with external organisations should be explicitly considered and measures required to manage the risks associated with this sharing put in place. Owners should be explicitly informed of the intention to share the information and who it is intended to share the information with. Permission to share the information should be required from the owners of the private information except where explicitly provided for by law.

285. The user should be provided with the ability to review, correct and withdraw their private information.

286. The service should be able to provide a subject, on request, a report that details the information held about them. Processes should be in place to enable any changes to that information to be made in order to maintain its accuracy.

Examples

287. Examples of services likely to fall into this category include those that offer a shopping capability, where the user is offered the facilities to store payment details to facilitate future purchases, are examples of Level 1 services:

Provision

288. Provision is likely to involve the use of standard features of commercially based systems.

Level 2 Privacy – Explicit

289. The system, of necessity, collects and collates private information that can be directly linked to an individual or legal entity. Misuse of the information collected could be perceived as, or could actually be, detrimental to the well being of the users.

Requirements

290. The mandatory minimum data handling measures defined in the Hanningan report [i] must be complied with (see also [j]).

291. A senior member of staff should be identified as the Information Asset Owner. The roles of the Information Asset Owner are defined in reference [k].

292. The service should be designed to minimise its privacy impact on prospective users. Privacy related objectives should be considered alongside business goals, and privacy considerations addressed at every stage of the service lifecycle.

293. The organisation providing the service should have an overall privacy policy/information charter. This policy should define the baseline privacy risk tolerance and appetite of the organisation. This document should be made available to the public.

294. An effective documented privacy management system should be in place to safeguard the private information collected. This should include an executive level representative appointed to be held accountable for proper management of the private information.

295. Privacy requirements should be considered at the outset of the project to deliver the service. The private information to be held by the service should be explicitly identified. A privacy impact assessment (PIA) should be performed in accordance with ICO's guidance [g]. The assessment should consider all aspects of privacy from the perspective of the individual rather than the organisation. The PIA should be subject to independent review and be signed off by the executive responsible for privacy.

296. Independent audit of compliance with the Data Protection Act and other relevant legislation should be performed.

297. The privacy risks identified should be managed throughout the life of the service. The process for managing these risks should be documented.(The privacy risks will be one factor in determining the appropriate security levels for the different security components)

298. A privacy policy/privacy impact assessment for the service should be placed in the public domain so that potential users of the service have access to it. Some of the information within the PIA report may be subject to security or commercial sensitivities. In such cases, it may be appropriate for the detailed information to be in confidential, appendices. Explicit details of the private information collected should be published. The purpose for which the information is collected should be explicitly defined. Details of the review, retention and deletion policy should be documented.

299. For on-line services, the user should maintain visibility of the private information that the service has collected directly from them. The user should be provided with the ability to review, correct and delete their private information.

300. The service should be able to provide a subject, on request, a report that details the information held about them. Processes should be in place to enable any changes to that information to be made in order to maintain its accuracy.

301. The policies should be fully resourced and effectively implemented. Compliance with the policies should be subject to regular independent review. Recommendations from the reviews and the actions it is proposed to take in response to any issues raised should be published.

302. The sharing of the private information within the organisation and with external organisations should be explicitly considered and measures required to manage the risks associated with this sharing put in place. Explicit permission to share the information will be required from the owners of the private information.

303. Any anonymisation of data performed should be subject to independent review by an appropriately qualified expert to ensure that the data has been effectively anonymised and is not susceptible to inference attacks. Removal of directly identifiable elements of records (e.g. user name, data of birth and address) may not be sufficient to ensure that the data is anonymous.

304. Accumulation and aggregation of data should not be performed. Note that where bulk data is held Level 3 privacy requirements should be met.

305. Access to the data should be strictly controlled and limited to those with a demonstrable need to know. Access rights should be minimised in respect of the following:

    a. the number of records accessible. The default should be that any member of staff has no access to protected personal information. If access is necessary, it should be to the smallest possible sub-set of records;

    b. the numbers of records viewed. The hierarchy should be no access / ability to view only aggregated data / ability to view only anonymous records / ability to view material from single identifiable records / ability to view material from many identifiable records simultaneously;

    c. the nature of information available. The hierarchy should be responses to defined queries (e.g. does X claim free school meals) without seeing the record / view of parts of the record itself / view of the whole record;

    d. the functionality, including searching, alteration, deletion, printing, downloading or transferring information.

306. Audit, monitoring, and accounting procedures should be in place to enable the detection of possible abuses of access rights provided to service personnel. This should making arrangements to log activity of data users in respect of

electronically held protected personal information, and for managers to check that logging is being properly conducted, with a particular focus on those working remotely and those with higher levels of functionality. Summary records of manager activity should be shared with the relevant Information Asset Owner and be available for inspection by the Information Commissioner's Office on request. The organisation should have forensic readiness policy in place to maximise their ability to preserve, analyse and use evidence from the system, should it be required.

307. If any element of the service that holds private information is to be carried out off shore, the guidance in CESG 'Good Practice Guide 6 - Outsourcing and Offshoring: Managing the Security Risks should be followed [l].

Examples

308. Government services that fall into this category include those where users may be identified and the actions recorded. The actions themselves have little significance to others. They include for example, applying for a motor vehicle tax disk, booking a driving test or registering a vehicle with DVLA.

309. Care would be needed with anything that could reveal a user's contact details and this would be seen as a serious breach of privacy even though the information itself is not particularly sensitive. Some individuals have a legitimate expectation that their location information is not made generally available.

Provision

310. A significant element of the required privacy controls will be implemented through personnel, physical and procedural controls. Technical controls are likely to exploit the standard security features of commercial based products (e.g. role based access controls to records).

Level 3 Privacy – Protected

311. Level 3 privacy requirements are applicable for systems holding bulk private data which is, of necessity, collected and collated

Requirements

312. The mandatory minimum measures data handling measures defined in the Hanningan report [i] must be complied with (see also [j]).

313. The service should be conceived and designed to minimise its privacy impact on prospective users. Privacy-related objectives should be considered alongside business goals, and privacy considerations addressed at every stage of the service's lifecycle. The system should be explicitly designed and implemented to counter the threat of internal staff abusing their access to the system.

314. The organisation providing the service should have an overall privacy policy/information charter. This policy should define the baseline privacy risk tolerance and appetite of the organisation. This document should be made available to the public.

315. A documented privacy management system should be in place to safeguard the private information collected. This should include appointment of an executive level representative to be held accountable for proper management of the private information.

316. Privacy requirements should be considered at the outset of the project to deliver the service. The private information to be held by the service should be explicitly identified. A rigorous detailed privacy impact assessment (PIA) should be performed. The assessment should consider all aspects of privacy from the perspective of the individual rather than the organisation. The physical, personnel, procedural and technical controls required should be identified. Systemic issues should be explicitly addressed. The PIA should be subject to independent review and be signed off by the executive responsible for privacy.

317. Independent external assessment of the service compliance with the Data Protection and other relevant legislation should be performed.

318. The privacy risks identified should be effectively managed throughout the life of the service. These risks will be one factor in determining the appropriate security levels for the different security components.

319. A privacy policy/PIA for the service should be placed in the public domain so that potential users of the service have access to it. Some of the information within the PIA report may be subject to security or commercial sensitivities. In such cases, it may be appropriate for distribution of detailed information to be limited. Explicit details of the private information collected should be published. The purpose for which the information is collected should be explicitly defined. Details of the review, retention and deletion policy should be published. The criteria for retention and deletion of data should be explicitly defined.

320. The policies should be fully resourced and effectively implemented. Compliance with the policies should be subject to regular independent review by an appropriate qualified external organisation. Recommendations from the reviews and the actions it is proposed to take in response to any issues raised should be published.

321. The sharing of the private information within the organisation and with external organisations should be explicitly considered and measures required to manage the risks associated with this sharing put in place.

322. Permission of the information owner should be obtained before information is released to an external organisation. Explicit confirmation that the external partners will provide the required protection to the information should also be obtained.

323. Granular, strong access control measures should be implemented to protect the data. Records should be marked with an access control list and a trusted mechanism used to enforce the controls defined. Access should be restricted to only those with legitimate requirement.

324. Access rights should be minimised in respect of each of the following:

    a. the number of records accessible. The default should be that any member of staff has no access to protected personal information. If access is necessary, it should be to the smallest possible sub-set of records;

    b. the numbers of records viewed. The hierarchy should be no access / ability to view only aggregated data / ability to view only anonymous records / ability to view material from single identifiable records / ability to view material from many identifiable records simultaneously;

    c. the nature of information available. The hierarchy should be responses to defined queries (e.g. does X claim free school meals) without seeing the record / view of parts of the record itself / view of the whole record; and

    d. the functionality, including searching, alteration, deletion, printing, downloading or exporting information.

325. Strict controls should be in place to prevent inappropriate aggregation by service provider staff.

326. Access to individual records should cause an audit trail to be produced that includes who accessed the record and the date and time of the access. An audit trail should also be kept of all deletions.

327. Monitoring and accounting procedures should be in place to enable the detection of possible abuses of access rights provided to service personnel. Alerting functionality should be considered for particular sensitive records. Inappropriate access should be treated as a disciplinary offence.

328. The service should be able to provide a subject, on request, a report that details the information held about them. Details of those with access to the record should be provided to the user on request. Processes should be in place to enable any changes to that information to be made in order to maintain its accuracy.

329. Any anonymisation of data performed should be subject to independent review by appropriately qualified experts to ensure that the data has been effectively anonymised and that effective measures to prevent inferences about a subject being drawn are in place (including identification of information not present in the data set). This includes reviewing any pseudonyms used to ensure that actual identities cannot be deduced. The risks associated with cross correlation of anonymised data should be carefully considered and adequately addressed. Removal of directly identifiable elements of records (e.g. user name, data of birth and address) may not offer sufficient protection.

330. The technical security measures in place to enforce the privacy controls should be subject to independent evaluation by appropriate technical experts.

Examples

331. Examples of systems that fall within this category include centralised electronic health record systems and centralised tax record systems.

Provision

332. Provision of services is likely to require privacy preserving top down design and implementation. Research in the design and implementation of effective systems is currently on-going and specialist security advice will be required. Implementations illustrating possible approaches to meeting the requirements include:

    a. the pilot implementation of the BMA Security policy for a hospital system for Hastings that was developed in 1995 [m]. Lessons learnt from the implementation are discussed in reference [n].

    b. NHS Connecting for Health's work on the electronic patient record. Their approach provided role based access controls. In order to access patient data a staff member should have a 'legitimate relationship'. In addition, a patient may declare part of their records to be 'sealed' or 'sealed and locked' further restricting access. In the first case, the sealed element of the record will be available to a particular care team, the existence of the sealed elements of the record will be visible to those with a legitimate relationship to the patient. In an emergency they will be able to break the seal and see the details. In the later case the part of the record that has been sealed and locked will only be visible to the particular care team [o].

Chapter 3 - Server Components

Key Principles

- Covers the application server security environments.
- The two server components defined are:
    - Information access – covering the unauthorised observation and manipulation of information. Levels defined increase with information sensitivity. Requirements, examples and provision guidance are provided.
    - Information availability – covering the means by which assurance is obtained. Reliability aspects are not covered. These components cover server confidentiality and availability concerns. Integrity issues are considered within the Business Logic components. Requirements, examples and provision guidance are provided.

Introduction

333. Server security components are those concerning application server environments. This section discusses these security components under the headings of:

    a. Information Access;

    b. Information Availability.

Information Access

334. Access related services address the unauthorised observation and manipulation of information that is received, stored, processed or disposed of within the server environment.

335. Four levels of access protection are defined that represent increasing levels of protection.

336. The organisational, personnel and physical security requirements of the organisations managing the servers are described in the Assurance security Components.

Level 0 Access – no specific measures

337. Level 0 is appropriate where none of the information handled in the server environment has any sensitivity and is therefore not subject to any formal access control policy except that required to ensure service continuity and data integrity.

338. Note that privacy requirements should always be met. Level 0 will not be appropriate if private information is collected by the system.

339. While private information is not being collected at this level, care should still be taken in designing the service to ensure that all malicious code insertion type attacks (e.g. SQL injection, cross site scripting) vulnerabilities have been considered to limit the opportunity for an attacker to exploit the service.

Requirements

340. There are no explicit requirements to provide information access protection within the server environment beyond those required to ensure service continuity and integrity. Care should still be taken to adopt good system practice.

Examples

341. Web services providing information to the general public may represent a service that may not require information access protection (though they may need higher levels of write access control to ensure data integrity and business continuity).

Provision

342. Standard commercial products are likely to be used to provide the required services. These will be configured and operated in accordance with normal good system practice. While no formal access controls are required to meet information access requirements, it should be noted that controls will be required to ensure the integrity and availability of the system.

Level 1 Access – self assessed commercial

343. At Level 1 the information processed and stored within the server environment will have some access limitations but will not attract a national protective marking. The impact of information disclosure is minimal. It is not appropriate where the server contributes to a service that attracts a Level 2 or 3 Privacy requirement.

Requirements

344. Appropriate organisational, personnel, physical and procedural controls should be in place to ensure the secure operation of the servers within the environment. The Assurance Security component gives more details of the requirements.

345. The design, configuration and operation of the system should be subject to review to ensure its secure operation. Self assessment is acceptable at this level. The Assurance Security component gives more details of the requirements.

346. The whole life cycle of the assets should be considered when determining the measures necessary to protect them. This includes putting appropriate measures in place to ensure their secure disposal (including the physical systems and media holding the data).

347. The system should offer access controls. These access controls should be configured to minimise the information and services that users have access to those necessary for them to perform their jobs effectively.

348. User registration and authorisation requirements for the back-office staff should be at least as stringent as those for the users of the service.

349. Users should be granted the minimum privileges necessary to perform their function. Privileged accounts should only be used by a user or administrator when performing functions that demand elevated privileges.

350. Access to the system should be via a secure logon process. The authentication requirements detailed earlier must be satisfied.

351. Access credentials issued should be unique to a particular user. Users must be instructed not to share credentials. Where shared credentials must be used to support for example, shift based working, other mechanisms should be in place to ensure activities can be traced to a specific individual.

352. Processes should be in place to regularly review the list of users with access to the system to ensure that all users with current access have a current business need.

353. Users should successfully authenticate themselves to the system before being able to access it. The type and strength of credential required should be determined in accordance with the guidance provided on Authentication.

354. The system should be hardened in line with commercial good practice. The services running on the system should be the minimum necessary to meet the business need.

355. A patch management process should be in place. This should ensure that patches to fix security vulnerabilities are tested and rapidly applied to the operational system.

356. Applications and utilities available on the system should be the minimum necessary to meet the business need.

357. Import and export controls should be in place. Only information object types that can be reasonably expected to be required to meet the business needs should be permitted to be imported on the system. Imports and exports should be

examined to confirm compliance with the policy and to confirm that they do not contain malicious content. A defined process should be documented for handling any malicious content received.

358. Server side validation of data input by services users should be performed to confirm that it conforms to expectations before being used to generate further outputs. Invalid data entry should be trapped and handled in a secure manner. Explicit consideration of malicious code insertion type attacks (e.g. SQL injection, cross site scripting) vulnerabilities should be given when designing the service.

359. Backup and archive data should be stored so that only authorised users have access to it.

360. The system should be designed to minimise the retention of sensitive information on untrusted client access devices.

361. An incident response plan should be in place. The incident response plan should cover:

    a. the assessment processes to assess the impact of an incident,

    b. processes required to ensure the controlled close down of elements of the system and controlled recovery processes to be followed.

362. This plan should be regularly tested to maintain its effectiveness.

Examples

363. Services that fall into this category are those for which the impact of disclosure of information is likely to be minimal. An example might be a service which enables a client to make an application or initiates a transaction that will be completed on the basis of a paper form. The service that allows the user to create and populate an electronic facsimile of the paper form will contain personal information that should be protected, but the information is only temporarily stored while the application is completed and is deleted on completion of the application (e.g. on-line completion of a passport application form).

Provision

364. At Level 1, commercial products are likely to be used to meet the requirements. The in-built security features of these products are likely to be sufficient to meet the security needs. The products will be configured and hardened in line with commercial good practice. For example, Windows Servers will be hardened in line with Microsoft hardening guidance [p]. Servers will be segregated in line with commercial good practice.

365. Access rights granted to users will be the minimum necessary to perform their business function. Only a minimum number of users will be granted administrative rights.

366. Standard system-provided activity monitors are likely to be used to regularly confirm that the system is operating in accordance with its expected parameters and to enable any suspicious activity or patterns of activity to be identified. Standard system-provided accounting logs will be reviewed by appointed security personnel for the system to ascertain whether there is any activity or pattern of activity that might indicate an unexpected electronic attack on the system. Account logs are likely to be reviewed at least monthly. Alerts are likely to be configured for critical events to ensure timely response.

367. Standard commercial tools will be used to check that the servers are correctly configured and that known vulnerabilities have been addressed. Automated tools are likely to be used to update the systems within the server environment. Product supplier websites, GovCertUK and other security bulletin boards are likely to be actively monitored to maintain awareness of potential server vulnerabilities.

368. Overall compliance with the security policy is likely to be audited at least annually.

Level 2 Access – assessed commercial

369. At Level 2 the information stored has access control requirements and may attract a protective marking of PROTECT (in lower risk environments). Impact of disclosure of the information is likely to be largely reputational with limited potential for individual harm. Bulk data loss may however have significant implications.

Requirements

370. At Level 2 the mandatory minimum security requirements specified by Hannigan apply [i].

371. All Level 1 Information access requirements apply at Level 2 as well. There are number of areas in which stronger controls are required. These are as follows:

    a. A risk assessment should be performed and the service accredited before entering service. HMG IA Standard 1 [q] is government preferred risk assessment method. HMG IA Standard 2 [r] provides details of central government approach to service accreditation.

    b. Equipment should be sited or protected to reduce the risks of unauthorised access. This includes providing protection of confidential information displayed on screens.

c. Equipment, information or software should not imported or be taken outside the secure environment without prior authorisation.

d. Any equipment taken outside the secure environment should be secured to account for the different risks associated with this.

e. Information written to media or printed out should be afforded an appropriate level of protection using physical, procedural and/or technical measures.

f. Strict controls should be in place to ensure that backup and archive material may only be accessed by authorised personnel.

g. Access controls should be used to minimise information accessible to a user to the minimum necessary to enable them to effectively perform their business role.

h. Commercial encryption products may be used to protect data in transit or data at rest. If encryption is used to protect data, the encryption product used should be either HMG or FIPS 140-2 and CCT Mark accredited. A plan should be in place to ensure the availability of the required key material and that access to key material is carefully controlled.

i. All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

j. Before any user of the server environment (e.g. system administrator, back-office staff) is allowed to access the system:

    i. their identity should be verified;

    ii. their business need to access the system should be confirmed;

    iii. they should have received appropriate training including security training;

    iv. they should have signed to confirm that they understand the relevant security policy and procedures and that they will abide by these procedures.

k. User rights to transfer data to removable media should be carefully considered and strictly limited to ensure that this is only provided where absolutely necessary for business purposes and subject to monitoring by managers.

l. Information import, export and disposal should be actively managed to minimise the information security risks. A risk assessment and business case should be produced for all import and export information types to be allowed. Import and exports resulting in high risks should not be allowed without a strong business case justifying their use being produced. This should be signed off by the Accreditor for the service.

m. Import and export controls should be in place. Imports should be scanned to confirm compliance with the import policy and to confirm that they do not contain a virus or other malicious content. Exports should be scanned to ensure that the export policy is complied with.

n. Applications capable of processing imported material should be configured to do so safely. For example, word processing and spreadsheet applications should disallow automatic macro execution without prior user permission. E-mails should not lead to the automatic download of objects. Free form user input should be pre processed to eliminate vectors for attacks such as SQL injection, XSS, etc.

o. Applications used to export data should be configured to do so safely. For example, 'hidden text' in word processing documents should be revealed to the user or removed before export.

p. Audit and accounting requirements are similar to Level 1, however, accounting logs should be afforded a higher level of protection and audits should be performed on a more regular basis. Automated analysis tools should be used to support the analysis of accounting data. Audit and accounting should meet at least the requirements of the Level 1 Situation Awareness Security Component. Audit and accounting logs should be protected to at least Information access and Internal Accountability levels 1.

q. Host based intrusion detection/prevent systems should be used in addition to the monitoring of standard system provided activity monitors, to ascertain whether there is any suspicious activity or pattern of activity that might indicate an electronic attack is being conducted.

r. All import requests should be recorded to meet specified audit requirements and to enable trend analysis to be performed.

s. The system design and security documentation should be subject to independent review by appropriate security experts. At least Level 1 Technical and Organisational Assurance are expected (see the Assurance Security component for more details of the requirement). Appropriate action should be taken to address any significant issues identified by these reviews.

t. Prior to the service going live an independent IT security health check should be performed by appropriate experts. Once the service has gone live independent IT security health checks should be performed after any significant change in system configuration and periodically (period to be agreed with the Accreditor) to confirm that the system remains secure. At least Level 1 Technical and Organisational Assurance are expected (see the Assurance security component for more details of the requirements.)

Examples

372. Examples of services that fall into this category are those that store private information that has little significance to others but whose unintended release would be embarrassing. They include for example, applying for a motor vehicle tax disk, booking a driving test or registering a vehicle with DVLA.

373. Care would be needed with anything that could reveal a users contact details and this would be seen as a serious breach of privacy even though the information itself is not particularly sensitive.

Provision

374. Provision of the services at Level 2 is similar to that at Level 1. The main areas of difference are that:

a. Products providing key elements of the security enforcing functionality are likely to have been subject to independent evaluation under Common Criteria [s]. The evaluated products are likely to have achieved at least EAL 2 accreditation. Encryption products used will have been subject to FIPS 140-2 [2] and CCT Mark evaluation [t]. Other products for which Common Criteria evaluation is inappropriate (e.g. anti-virus) will have been subject to CCT Mark testing.

b. Security documentation produced is likely to be in line with HMG IS 2 [r] (or an equivalent) and agreed with the Accreditor before the system goes live. This documentation will be subject to regular review and will be updated as required.

c. Audit and accounting should be performed on a regular basis. Accounting logs are likely to be reviewed at least weekly. Alerts will be configured for critical events to ensure timely response.

d. The configuration of the system will have been subject to independent audit by relevant security experts (e.g. CHECK[u] or CREST [v] approved suppliers).

[2] The recommended IPS 140-2 profile is specified in [w].

e. Compliance reviews of the system with security policy will be performed at least annually.

Level 3 Access – assessed government

375. At Level 3 the information stored has strong access control requirements and may attract a protective marking of PROTECT (in higher risk environments) or RESTRICTED for subsets of the data or in bulk. The impact of unwarranted access is likely to be significant with scope for individual harm. Bulk data exposure could carry significant reputational and business impact.

Requirements

376. All Level 2 access control requirements apply at Level 3 as well. There are number of areas where stronger controls are required. These are as follows:

a. User registration and authorisation requirements for the back-office staff will be at least as stringent as those for the users of the service and will comply with the requirements specified in CESG Information Assurance Memorandum 26 [c].

b. Segregation of duties should be implemented between those with security responsibilities and those with system administration responsibilities.

c. The servers should be hardened in line with government good practice. A risk assessment and business case should be produced for all services which it is proposed to run in the server environment.

d. Import and export controls should limit imports and exports to only those information object types that can be explicitly justified. A risk assessment and business case should be produced for all import and export requirements.

e. Strict controls should be in place to protect data at rest to ensure that it may only be accessed by authorised personnel. If encryption is used, an HMG Baseline Grade approved product should be used. This should be configured and operated in accordance with its agreed security operating procedures and HMG IA Standard 4 [w]

f. Disposal of data should be performed in accordance with HMG IA Standard 5 [x].

g. Strong accounting and audit is required. This should be implemented in accordance with CESG Good Practice Guide 13 [y] It should be sufficient to ensure that all users can be held accountable for their actions.

h. Level 2 or Level 3 Situational Awareness should to have been implemented. The capability to carry out display and detailed data mining and analysis of accounting records should have been provided.

i. The system design and security documentation should be subject to independent review by appropriate security experts. Level 2 Technical and Organisational Assurance is expected (see the Assurance Security component for more details of the requirement). Appropriate action should be taken to mitigate any significant issues identified by these reviews.

j. Prior to the service going live an independent IT security health check should be performed by appropriate experts. Once the service has gone live independent IT security health checks should be performed after any significant change in system configuration and periodically (period to be agreed with the Accreditor) to confirm that the system remains secure. Level 2 Technical and Organisational Assurance is expected (see the Assurance security component for more details of the requirements).

Examples

377. Example services for which level 3 information access is appropriate include:

a. electronic filing of income tax and Value Added Tax (VAT) returns;

b. services that give access to sensitive private information, for example a personal medical record.

Provision

378. Provision of the services at Level 3 is similar to that at Level 2. The main areas of difference are as follows:

a. All personnel with physical access to the system are likely to have been vetted in accordance with BS requirements (or equivalent). Personnel with more privileged access, for example system administrators, are likely to have been subject to SC vetting.

b. The location at which the servers are located is likely to be a site approved for handling protectively marked information.

c. Boundary protection devices, network devices and servers will all be hardened in accordance with HMG IA good practice. The approach adopted involves disabling all services and then enabling the minimum set of services required in order to meet the business requirements.

d. Network zoning is likely to be used to support data separation and support access control restrictions.

e. Network based intrusion detection systems are likely to have been deployed at key nodes with the server environment. Host based intrusion detection systems are likely to have been implemented on critical servers.

f. Incident response procedures will have been established. A fully resourced computer incident response team is likely to have been stood up. Incident recovery procedures, controlled close down, impact assessment and recovery procedures will be documented and regularly tested. Incidents would be reported to GovCertUK and CINRAS.

g. The system design and security documentation is likely to have been subject to independent review by CESG, CLAS Consultants or CTAS approved supplier and appropriate action taken to mitigate any significant issues identified. The service configuration is likely to be subject to regular independent health check by CESG, a CHECK approved supplier or a CTAS approved supplier [z]. This will be at least annually and after any significant system configuration change.

Information Availability

379. This security component covers the means by which assurance is obtained that access to information and resources cannot be withheld in an unauthorised manner. This section does not address reliability aspects in general, its specific focus is denial of authorised access to resources as a result of malicious activity and the susceptibility of systems and services to such threats.

380. The organisational, personnel and physical security requirements of the organisations managing the servers are described in the Assurance requirements.

Level 0 Availability – no specific measures

381. No explicit specific requirements for controls to be required to block Denial of Service attacks over and above reasonable expectations of continuing service delivery.

382. The reputational issues should be considered in the attention given to availability. Though the damage to the individual requesting the service many be minimal, the impact of failure to address susceptibility to attack may damage the credibility of the service provision.

Requirements

383. Normal good system practice should be adopted in respect of designing, implementing and managing the system. It is likely that at Level 0 no explicit availability measures are necessary.

384. No special measures need be taken to ensure data backup or continuity of service following an interruption to service. In particular, no special measures need to be taken to recover partially completed transactions, other than for those that affect the integrity of existing information.

Examples

385. Examples of transactions that might merit Level 0 availability services include:

a. a client reads or downloads publicly available information from a government website. Unavailability of the information would cause at most minimal inconvenience to the client, who could attempt to access the information at a later date.

b. a client e-mails a government department with a request for general information and expects the material to be returned via e-mail. Failure of the service would cause the client to experience at most minimal inconvenience. The Client could re-submit the request at a later date.

Provision

386. Standard commercial products are likely to be used to provide the required services. These will be configured and operated in accordance with normal good system practice.

Level 1 Availability – commercial

387. At Level 1 attention needs to be paid to hardening the servers against Denial of Service (DoS) attacks but the service criticality is not such as to justify bespoke measures or severe restrictions on service delivery.

388. Standard commercial good practice is sufficient to ensure that the system meets its Service Level Agreement (SLA). A guaranteed process exists for recovering the service in the event of a service outage.

Requirements

389. Personnel, procedural, physical and access controls that meet the requirements of the Level 1 Information Access Security Component are expected to be in place.

390. A good commercial system architecture design should be used. Fault tolerant components are likely to be used to ensure service availability (e.g. redundant processor configurations, RAID arrays, redundant power supplies) although they are not mandated.

391. The design, implementation and operation of the system should be subject to independent review. At least Level 1 Organisational Assurance and Technical Assurance are expected at this level.

392. SLAs for externally provided services should be set to meet the availability requirements (including transaction availability).

393. Careful consideration should be given to sizing of the communications and information servers so as not to compromise availability. The sizing should be based on realistic estimates of demand for the service.

394. Alternative communications paths that can be switched in within the timescale appropriate to the business need should be available.

395. UPS should be provided to allow 'soft' failure with power recovery achievable within a timescale appropriate to the business need.

396. A configuration management plan and processes covering the communications and information systems providing the service should be designed and implemented.

397. Formal configuration and change management process should be in place. Configuration changes should be approved by the system manager before implementation and should be subject to secure audit (technical or procedural). Software should only be introduced with the approval of the system manager and a full inventory of all hardware and software and a network diagram showing all approved connections should be maintained.

398. A failure impact analysis should be carried out and recorded for all information and communication system components. This should be reviewed in the event of significant configuration changes. No upgrades should be permitted without prior assessment.

399. A controlled connection closedown process should exist that allows essential business processes to be maintained in the presence of significant Denial of Service attacks.

400. A process should be available to provide access in the event of loss of a password, access token or cryptographic key.

401. A business continuity plan should be in place and subject to regular review and testing. The plan should address:

    a. management roles and responsibilities for business continuity;

    b. recovery procedures and audit trail;

c. security specific recovery actions.

402. Backups should enable restoration of all relevant information to be recovered within a time window required by the business need. The backup and restoration process should be documented.

403. Cryptographic checksums or secure software isolation for system software, configuration data and storage facilities should be provided The backup should be compared against the original before the backup media is stored offsite. The restoration process should be documented and tested regularly. A secure self-test process should be undertaken regularly using these facilities.

404. Commercial good practice self test processes should be in place to enable the health of the system to be validated.

405. Audit and accounting should be performed in accordance with Level 1 or higher Situational Awareness Security Component.

406. The service levels provided by the service should be regular reviewed to confirm that the SLAs are being met. System performance and usage should be monitored to ensure continued service availability and to enable future service needs to be anticipated.

Examples

407. Level 1 availability is likely to apply to the majority of e-government services for which short term unavailability of service or information is an inconvenience to users though unlikely to cause harm but where the reputation of the department might be undermined if the service is seen as vulnerable to attack.

Provision

408. Provision of the service is likely to involve the use of standard commercial products. A degree of fault tolerance will be implemented through the use of standard commercial products (e.g. server clustering, use of servers with redundant components, use of UPS, RAID, etc.). Specialist, high availability fault tolerant components are unlikely to be necessary at this level.

409. Access rights granted to users will be the minimum necessary to perform their business function. Only the minimum number of users will be granted administrative rights. Access rights will be kept under review and updated when user requirements change.

410. Import controls are likely to be based on blacklisting. Procedural controls are likely to be used to control the import of objects from media (e.g. CDs). Mail and other electronic imports are likely to be screened automatically at the gateway to the system. Dangerous file types (e.g. executables) are likely to be

automatically blocked or quarantined at the gateway. The list of file types to be blocked or quarantined is likely to be based on a blacklisting approach. Data that is likely to be reasonably required by the business will be allowed by default.

411. The communications across the gateway will be minimised to those that are reasonable required by the business. Filtering technology is likely to be used to remove SPAM, SPIT and SPIM. All imported and exported objects will be subject to anti-virus scanning using a commercial anti-virus product. An anti-virus strategy will be in place to ensure the timely update of anti-virus signatures.

412. Standard system provided activity monitors are likely to be used to regularly confirm that the system is operating in accordance with its expected parameters and to enable any suspicious activity or patterns of activity to be identified. In addition to automated scanning, standard system-provided accounting logs will be reviewed by appointed security personnel for the system to ascertain whether there is any activity or pattern of activity that might indicate an unexpected electronic attack on the system. Account logs are likely to be reviewed at least monthly. Alerts are likely to be configured for critical events to ensure a timely response. Accounting logs will be retained to enable a record of transaction times and record changes. Access to the logs will be controlled to minimise the risk of tamper.

Level 2 Availability – critical

413. At Level 2 there is a requirement for specific attention to be paid to hardening the servers against Denial of Service attacks, possibly at the cost of reduced provision of richer functionality in the interest of reducing the attack ‘surface’.

Requirements

414. Personnel, procedural, physical and access controls that meet the requirements of the Level 2 Information Access Security Component are expected to be in place.

415. The availability requirements should be set to be compatible with the assessment of the business need. SLAs for externally provided services should be set to meet the availability requirements (including transaction availability).

416. A good commercial system architecture design should be used. This will have been designed to prevent, detect and tolerate some level of malicious and non-malicious attack.

417. The design, implementation and operation of the system should be subject to independent review. At least Level 2 Organisational Assurance and Technical Assurance are expected at this level.

418. The system design and security documentation should be subject to independent review by appropriate security experts. Level 2 Technical and Organisational Assurance is expected (see the Assurance Security component for more details of the requirement). Appropriate action should be taken to mitigate any significant issues identified by these reviews.

419. Prior to the service going live an independent IT security health check should be performed by appropriate experts. Once the service has gone live independent IT security health checks should be performed after any significant change in system configuration and periodically (period to be agreed with the Accreditor) to confirm that the system remains secure. Level 2 Technical and Organisational Assurance is expected (see the Assurance security component for more details of the requirements).

420. Failure impact analysis should have been carried out and recorded for all information system and communication components. This should be reviewed in the event of significant configuration changes.

421. Careful consideration should be given to sizing of the communications and information systems. The sizing should be based on realistic estimates of demand.

422. User registration and authorisation requirements for the back-office staff will be at least as stringent as those for the users of the service and will comply with the requirements specified in CESG Information Assurance Memorandum 26 [c].

423. Segregation of duties should be implemented between those with security responsibilities and those with system administration responsibilities.

424. A configuration management plan and processes covering all the elements within the server environment should be in place. Configuration changes should be approved by the system manager before implementation and should be subject to full testing before they are applied to the operational system, including security testing. Software should only be introduced with the approval of the system manager and a full inventory of all hardware and software and a network diagram showing all approved connections should be maintained. Introduction of new software should be subject to full testing (including security testing) within the test environment before being applied to the operational system.

425. Server environments should be configured to enforce access controls and limit exposure only to applications with a specific operational business function. Access control should be configured to ensure that user access is limited to the services for which they have a need to know. The servers should be hardened in line with government good practice. A risk assessment and business case

should be produced for all services it is proposed to run in the server environment.

426. Import controls should limit import to only those that can be explicitly justified. A risk assessment and business case should be produced for all import requirements.

427. Strong accounting and audit is required. This should be implemented in accordance with CESG Good Practice Guide 13 [y]. The auditing should be sufficient to ensure that all users can be held accountable for their actions.

428. Level 2 or Level 3 Situational Awareness should to have been implemented. The capability to carry out display and detailed data mining and analysis of accounting records should have been provided.

429. Back up and archive of data should be performed. This should enable restoration of all relevant information to within a period determined by the business need.

430. The backup should be compared against the original before the backup media is stored offsite. The restoration process should be documented in the business continuity plan and tested regularly.

431. Baseline level cryptographic checksums or secure software isolation for system software, configuration data and storage facilities should be provided. A secure self-test process should be undertaken regularly using these facilities.

432. Service performance and usage should be monitored to ensure are operating within expected parameters and to enable future service requirements to be anticipated.

433. A commercial good practice self test process should be in place to enable the health of the service to be confirmed.

434. A business continuity plan should be in place and subject to regular review. The business continuity plan should be subject to regular rehearsal. The plan should address:

    a. management roles and responsibilities for business continuity;

    b. recovery procedures and audit trail, covering the system, communications and transactions;

    c. security specific recovery actions.

Examples

435. Examples of services that fall into this category are those for which penalties exist for late provision of data to government, such as electronic filing of income tax returns, PAYE returns and Value Added Tax (VAT) returns.

Provision

436. Commercial good practice for a critical service is likely to be followed. The architecture for the system will have been designed to prevent, detect and tolerate some level of malicious and non-malicious attack. This could include, for example, use of boundary protection devices, import filtering, hardened operating systems and network components, etc. to minimise the attack 'surface'. Multi-tier, high redundancy architectures (e.g. redundant processor configurations, mirrored disks, RAID arrays) and geographical distribution are likely to be exploited. Hot or warm stand-by systems may be needed to meet the business need. Alternative communications paths with immediate failover may also be necessary.

Chapter 4 - Network Components

Key Principles

- Covers the network security measures necessary to protect information in transit between the online public service and the user of the service.
- Five aspects of security covered; Communications Security, Network Authentication, Network Protection, Situational Awareness and Business Logic Components.
- Levels ascend in order of security measures required, often compounding on previous lower level, where appropriate. Levels defined are not linear across all security aspects.

Introduction

437. The network security components cover the measures necessary to protect information in transit between the online public service and the user of the service. Four aspects of security are considered within this area, namely:

    a. Communications security;

    b. Network authentication;

    c. Network protection;

    d. Situational awareness;

    e. Business Logic Components.

Communications Security

438. Communication security covers the measures by which assurance is gained observation or modification of information cannot occur in transit to and from the servers used to host the service. It typically relates to the requirements for encryption of communication links.

439. The organisational, personnel and physical security requirements of the organisations managing the network are described in the Organisational Assurance Security Component (see Chapter 5).

440. Four levels of communications security are defined.

Level 0 Communications Security – no specific measures

441. At Level 0 there are limited requirements for technical communication security measures. This could be because the information to be exchanged over the

network is not sensitive. Alternatively it could be because strong physical, procedural and personnel controls are in place provide adequate protection.

Requirements

442. At Level 0 there are no explicit communications security requirements.

Examples

443. Examples of transactions that might merit level 0 Communications security defence include:

    a. A client reads or downloads publicly available information from a government web site.

    b. A client e-mails a government department with a request for general information and expects the material to be returned via e-mail. Electronic attack resulting in, for example, loss of integrity of the information might result in minimal inconvenience or loss of time to the client, but no serious consequences such as risk to safety.

Provision

444. At Level 0 there are limited requirements for technical communications security measures. This could be because the information is non-sensitive, the physical, procedural and personnel security measures provider by the network provider are sufficient to meet the security requirements or because the information is protected at the transaction level.

Level 1 Communications Security – limited

445. At Level 1 the threat and vulnerability analysis leads to a requirement for explicit communication security measures to be implemented. The analysis does not however identify a requirement for strong measures that are able to resist a highly capable attacker.

Requirements

446. Communications across the network should be encrypted to protect their confidentiality and integrity.

Examples

447. Example of service that might attract Level 1 communications security measures include:

    a. A client arranges a meeting with a government official by email. The impact of loss of confidentiality or integrity or other consequences of electronic attack is inconvenience and lost time, possibly minor financial loss, but no lasting impact on either party.

b. A client requests medical appointments which are considered personal and need clinical confidentiality.

c. A client purchases a low cost government publication over the Internet. The impact of malicious electronic attack to attribute the purchase to the wrong client, or to alter the number of copies ordered, for example, would be inconvenience and possibly refunding or recovering incorrect payments.

448. The most significant threats to the service at this level are anticipated to come from opportunistic attackers and from threat sources with some IT knowledge and the resources to implement simple network attacks only. Most capable attackers are assumed not to be motivated to attack the service.

Provision

449. Provision is likely to be through the use of standard commercial products, for example, the use of TLS or IPSEC.

Level 2 Communications Security – significant

450. At level 2 the threat and vulnerability analysis leads to a requirement for explicit communication security measures. The threat actors identified are assessed to have a significant capability to attack the service but are not assumed to include well resourced and capable foreign intelligence services.

Requirements

451. Communications across the network should be encrypted to protect their confidentiality and integrity. The encryption product used should have been subject to independent validation to confirm its correct design, implementation and operation.

452. Switches, routers and other network devices should be hardened in line with Network Protection Level 2 or 3.

Examples

453. Examples of transactions that might merit level 2 Communications security include:

a. A client completes an income tax return online. Electronic attack might result in details of the income tax assessment being released to an unauthorised third party.

b. A client undertakes a financial transaction. Electronic attack resulting in disclosure of a debit card number, for example, would be likely to cause significant distress and inconvenience to a client.

454. The threat analysis for these services leads to a requirement for explicit communication security measures to counter the threats identified. The threats identified are assessed to have a significant capability to attack the service but are not assessed to include well resourced and capable Foreign Intelligence Services.

Provision

455. Communications security is likely to be implemented through the use of commercial products whose cryptographic modules have been accredited to be FIPS 140-2[3] compliant by an FIPS 140 test laboratory. The preferred FIPS 140-2 profile is specified in HMG IA Standard 4. Products containing only CESG approved algorithms are preferred. The products should also have achieved CCT Mark accreditation [t]

Level 3 Communication Security – substantial

456. At level 3 the threat analysis indicates that strong measures are required to counter well resourced and competent attackers.

Requirements

457. Communications across the network should be encrypted to protect their confidentiality and integrity. An HMG Baseline Grade encryption product should be used. This should be operated in accordance with its CESG approved security operating procedures and HMG IA Standard 4 [a].

458. Switches, routers and other network devices should be hardened in line with Network Protection Level 3.

Examples

459. Examples of service that might merit level 3 communications security protection include:

    a. Electronic procurement services used by Defence and FCO organisations that attract a RESTRICTED protective marking;

    b. Electronic travel services used for booking travel for VIPs;

    c. the provision of threat information from government to organisation that form part of the Critical National Infrastructure;

    d. the provision of information regarding the status of a criminal investigation.

[3] The recommended FIPS 140-2 profile is provided in [w].

460. At this level the threat analysis suggests the need for strong measures to counter well resourced and competent adversaries.

Provision

461. HMG Baseline Grade network products are used to encrypt data prior to its transfer on to the network. These products are configured and operated in accordance with the approved security operating procedures and HMG IA Standard 4.

462. Switches and routers are hardened in accordance with the Network Protection Level 3.

Network Authentication

463. Network Authentication covers the means by which assurance is obtained of the authenticity of machines involved in inter domain connections and data exchanges. Two levels of authentication have been identified.

Level 0 Authentication – limited

Requirement

464. This level covers the situation where there is a low threat or limited opportunity for attack

465. There are no explicit requirements other than those imposed by duty of care requirements.

Examples

466. An example of a situation in which limited authentication would be acceptable is when connecting two government e-mail servers that are hosted on the Government Secure Internet. In this case use of network identifiers to identify the relevant server is acceptable due to the low level of risk of spoofing on the accredited network.

Provision

467. The physical, procedural and personnel security measures associated with the network are sufficient to counter the threat of network spoofing. Alternatively transaction/application level security measures may be being used to protect communications, negating the requirements for network level authentication.

468. If network authentication is required, it will be sufficient to rely on a network identifier, such as IP address, MAC address or URL. Spoofing of these identifiers will have been assessed as low risk for the gGovernment service.

Level 1 Authentication – active

469. At Level 1 threat analysis suggests that there is a reasonable risk of spoofing and that robust measures to prevent capture and misuse of the authenticator are justified.

Requirements

470. A two way authentication process should be followed.

471. A strong authentication mechanism should be used i.e. authentication should be cryptographically based and use an approved challenge response protocol. Protection against man-in-the-middle attacks should be provided.

Examples

Services that are handling private information that do not provide end-to-end application level protection will require Level 1 Network Authentication.

Provision

472. At Level 1 cryptographic techniques are used to authenticate the network devices. This could, for example involve the use of pre-placed symmetric keys of appropriate length. Alternatively public key cryptography could be used, using for example TLS or IPSEC implementations. FIPS-140 or CESG evaluated cryptographic products will be used. HMG IA Standard 4 provides guidance on the selection of the appropriate grade of device.

Network Protection

473. Network protection provides the means to assure that the service is protected from an adversary with some degree of unconstrained network access.

Level 0 Protection – no specific measures

474. At Level 0, no special measures beyond the requirement for duty of care in the application of common commercial measures are needed.

Requirements

475. There are no explicit requirements.

Examples

476. Level 0 Network protection is appropriate for transactions in which minimal damage might arise from a network attack. For example, a network service that enables publicly available information to be downloaded from a government site and for which the results of an attack would be minimal inconvenience to the user of the service.

Provision

477. At Level 0, standard commercial network services are likely to be used.

Level 1 Protection – baseline

Standard commercial good practice measures are taken to minimise network access and import and export. The controls are subject to self-assessment against the perceived threat and hence an acceptable response.

Requirements

478. Appropriate organisational, personnel, physical and procedural controls should be in place to ensure the secure operation of the network services. The Assurance Security component gives more details of the requirements.

479. The design, configuration and operation of the system should be in accordance with good commercial practice and should be subject to review to ensure its secure operation. Self assessment is acceptable at this level. The Assurance Security component gives more details of the requirements.

480. The whole life cycle of the assets should be considered when determining the measures necessary to protect them. This includes ensuring that appropriate measures are in place to ensure their secure disposal (including the physical systems and media holding the data).

481. Access controls should be in place to ensure that only trusted individuals with a legitimate business need have access to the network assets.

482. User registration and authorisation requirements for the network administration staff should be at least as stringent as those for the users of the service.

483. Users should be granted the minimum privileges necessary to perform their function.

484. Access to the system should be via a secure logon process. The authentication requirements detailed earlier must be satisfied.

485. Access credentials issued should, as far as possible, be unique to a particular user. User should be instructed not to share credentials.

486. Processes should be in place to regularly review the list of users with access to the system to ensure that all users with current access have a current business need.

487. Users should successfully authenticate themselves to the system before being able to access it. The type and strength of credential required should be determined in accordance with the guidance provided on Authentication.

488. Network components should be hardened in line with commercial good practice. The services running on the system should be the minimum necessary to meet the business need.

489. System configuration should be under proper control and unauthorised entities should be prevented from accessing and modifying important configuration data such as DNS, network addressing and routing structures.

490. There should be an effective configuration management process and routine inspections to ensure cross domain services and interfaces are limited to those necessary to meet the connection's business objectives.

491. Network import and export controls should be in place. Only information object types that can reasonably be expected to be required to meet the business needs should be allowed across the network boundary. All imported objects should be screened to confirm that they conform to the import policy and that they do not contain viruses or other malware. An anti-virus strategy will be in place to ensure the timely update of anti-virus signatures.

492. System responses in the event of a service being refused (or permitted) should be designed so as to prevent anyone from deducing any information that might be used to attack the system.

493. A patch management process should be in place. This should ensure that patches to fix security vulnerabilities are rapidly applied to the operational system.

494. Audit and accounting should be performed in accordance with commercial good practice. This should meet at least the requirements of the Level 1 Situational Awareness Security component. Audit and accounting logs should be protected to at least Server - Information Access Level 1.

495. An incident response plan should be in place. The incident response plan should cover the assessment processes to assess the impact of an incident, processes required to ensure the controlled close down of elements of the network when required and the recovery process to be followed. Security staff should examine all incidents of electronic attack and determine whether additional countermeasures should be put in place.

Examples

496. Examples of services that might merit level 1 network protection include information services for which loss of integrity or other consequence of electronic attack is inconvenience and lost time, possible with minor financial loss, but no lasting impact on any of the parties involved in the transactions.

Provision

497. At Level 1 commercial products will be used to meet the requirements.

498. Boundary protection devices will be used to limit the types of traffic flowing into and out of the network. These devices will be configured to minimise the traffic types allowed across the boundary. Traffic traversing the boundary will be subject to content scanning to confirm that it conforms to permitted types, to ensure the removal of viruses and other malware and to eliminate unwanted mail. Web traffic filtering will be performed to prevent the browsing of inappropriate content and to remove dangerous mobile code. SPIT and SPIM filtering will be performed if necessary.

499. The types of traffic allowed will be based on those reasonably required by the business. A risk assessment will have been performed to inform the selection of allowable traffic. Dangerous traffic types are blocked by default.

500. Network zoning will have been performed to provide a basic level of data separation on the network. Voice, data and management traffic will be segregated where possible.

501. Network devices will have been hardened in line with commercial good practice. This will include, for example,

    a. Removing or disabling all services not needed;

    b. Enabling strong passwords on all interfaces;

    c. Limiting management capabilities to the minimum necessary;

    d. Configuring privilege levels;

    e. Limiting remote access as far as possible;

    f. Limiting local access as far as possible;

    g. Displaying a login banner;

    h. Ensuring SNMP is configured securely;

    i. Ensuring anti-spoofing is configured;

    j. Ensuring Denial of Service attacks mitigations are configured.

    k. Enabling logging and NTP.

502. The configuration of the devices will be subject to review. These reviews do not however need to be performed by external independent specialists.

503. The accounting logs will be regularly reviewed to enable the detection of attacks on the system. Alerting on critical events will be implemented. Standard network activity monitoring tools are likely to be regularly used to confirm that the system is operating in accordance with its expected parameters and to enable any suspicious activity or patterns of behaviour to be detected.

504. Standard commercial tools will be used to check that network devices are correctly configured and that known vulnerabilities have been patched. Supplier websites, GovCertUK and other security bulletin boards are likely to be actively monitored to maintain awareness of current threats and vulnerabilities and the recommended actions to be taken in response to them.

505. Overall compliance with the security policy is likely to be audited at least annually.

Level 2 Protection – enhanced

506. An independent assessment is made of the threat and vulnerabilities. The response is shown to be reasonable and proportionate.

507. Standard commercial good practice measures are taken to minimise network access, import and export and service monitoring. Standard commercial products are used to provide protection.

Requirements

508. All Level 1 network protection requirements apply at Level 2 as well. There are a number of areas in which stronger controls are required.

    a. The organisational Assurance and Technical Assurance for the network service will be at least Level 1.

    b. A risk assessment should be performed and the service accredited before entering service. HMG IA Standard 1 [q] is government preferred risk assessment method. HMG IA Standard 2 [r] provides details of central government's approach to service accreditation.

    c. Equipment should be sited or protected to reduce the risks of unauthorised access.

    d. Before any user of the network environment (e.g. network administrator) is allowed to access the system:

        i. their identity should be validated;

        ii. their business need to access the system should be confirmed;

iii. they should have received appropriate training including security training;

iv. they should have signed to confirm that they understand the relevant security policy and procedures and that they will conform to these procedures.

e. Information import and export should be actively managed to minimise the information security risks. Services through boundary protection devices are blocked by default with an explicit risk and business case being made for each allowed service.

f. Audit and accounting requirements are similar to Level 1, however, accounting logs will need to be afforded a higher level of protection and audits should be performed on a more regular basis. Accounting logs should be protected to at least Information access and Internal Accountability levels 1. Automated analysis tools should be used to support the analysis of accounting data.

g. Network based intrusion detection/prevent systems should be used in addition to the monitoring of standard system provided activity monitors, to ascertain whether there is any suspicious activity or pattern of activity that might indicate an electronic attack is being conducted. Abnormal traffic patterns are likely to be blocked by default.

h. Prior to the service going live an independent IT security health check should be performed by appropriate experts. Once the service has gone live independent IT security health checks should be performed after any significant change in system configuration and periodically (period to be agreed with the Accreditor) to confirm that the system remains secure. At least Level 1 Technical and Organisational Assurance are expected (see the Assurance security component for more details of the requirements.)

Examples

509. Examples of services that might merit level 2 network protection include:

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

b. A client undertakes a financial transaction. Electronic attack might result in disclosure of credit or debit card details, causing significant distress and inconvenience to the client.

Provision

510. Provision of the services at Level 2 is similar to that at Level 1. The main areas of difference are that:

    a. Products providing key elements of the security enforcing functionality are likely to have been subject to independent evaluation under Common Criteria. The evaluated products are likely to have achieved at least EAL 2 accreditation. Encryption products used will have been subject to FIPS 140-2[4] and CCT Mark evaluation. Other products for which Common Criteria evaluation may be inappropriate will have been subject to CCT Mark testing.

    b. All components will be hardened in line with commercial good practice.

    c. Service minimisation, import controls and export controls will be more rigorously enforced and actively managed.

    d. Audit and accounting is performed on more regular basis. Accounting logs are likely to be reviewed at least weekly. Alerts are configured for critical events to ensure a timely response.

    e. The configuration of the system will have been subject to independent audit by relevant independent security experts.

Level 3 Protection – significant

511. At Level 3 there is a requirement for strong controls on network access. An independent assessment by informed government assessors is carried out. Privileged sources are used to inform the threat assessment. The mitigating measures may include government capabilities and services and result in restrictions on the service to minimise exposure.

Requirements

512. All Level 2 network protections requirements apply at Level 3 as well. There are a number of areas in which stronger controls are required. These are as follows:

    a. User registration and authorisation requirements for the back-office staff will be at least as stringent as those for the users of the service and will comply with the requirements specified in CESG Information Assurance Memorandum 26 [c].

    b. Segregation of duties should be implemented between those with security responsibilities and those with system administration responsibilities.

[4] The preferred evaluation profile is specified in [w].

c. The network components should be hardened in line with government good practice. A risk assessment and business case should be produced for all services which it is proposed to run in the server environment.

d. Import and export controls should limit import and exports to only those that can be explicitly justified. A risk assessment and business case should be produced for all import and export requirements.

e. Strong authentication mechanisms should be used to access the network devices. Access control should be configured to ensure that network operators' access is limited to the information for which they have a need to know.

f. If encryption is used, an HMG Baseline Grade approved product should be used. This should be configured and operated in accordance with its agreed security operating procedures and HMG IA Standard 4 [w]

g. Strong accounting and audit is required. This should be implemented in accordance with CESGHMG Good Practice Guide 13 [y]. It should be sufficient to ensure that all users can be held accountable for their actions.

h. Level 2 or Level 3 Situational Awareness should to have been implemented. The capability to carry out display and detailed data mining and analysis of accounting records should have been provided.

i. The system design and security documentation should be subject to independent review by appropriate security experts. Level 2 Technical and Organisational Assurance is expected (see the Assurance Security component for more details of the requirement). Appropriate action should be taken to mitigate any significant issues identified by these reviews.

j. Prior to the service going live an independent IT security health check should be performed by appropriate experts. Once the service has gone live independent IT security health checks should be performed after any significant change in system configuration and periodically (period to be agreed with the Accreditor) to confirm that the system remains secure. Level 2 Technical and Organisational Assurance is expected (see the Assurance security component for more details of the requirements).

Example

513. Examples of transaction that might merit level 3 network protection include:

a. Transactions involving transfer of medical records. Electronic attack might result in the disclosure of client medical information to an unauthorised third party, or loss of integrity that might cause substantial distress and/or risk to the health of the client;

b. Transactions involving the transfer of income tax assessment returns. Electronic attack might result in details of the income tax assessment being released to an unauthorised third party causing substantial distress

c. Transactions involving the transfer of PAYE and VAT returns. Electronic attack might result in the release of commercially sensitive and/or private information to third parties and possible substantial inconvenience and financial loss.

Provision

514. Provision of the services at Level 3 is similar to that at Level 2. The main areas of difference are as follows:

a. All personnel with physical access to the system are likely to have been vetted in accordance with BS requirements. Personnel with more privileged access, for example network administrators, are likely to have been subject to SC vetting.

b. The location at which the active network devices are located is likely to be at sites that have been approved for handling information with a National protective marking.

c. Boundary protection devices, network devices and network management devices will all be hardened in accordance with government good practice. Only those services, protocols, ports and addresses that are explicitly required will be allowed. Everything else will be denied. All unnecessary services will have been disabled.

d. Network zoning is likely to be used to support data separation and support access control restrictions. This includes the separation of voice, data and management traffic.

e. Level 2 or Level 3 Situational Awareness is likely to have been implemented. The capability to carry out display and detailed data mining and analysis of accounting records will have been provided.

f. Network based intrusion detection/prevent systems should be used in addition to the monitoring of standard system provided activity monitors, to ascertain whether there is any suspicious activity or pattern of activity that might indicate an electronic attack is being conducted. Government attack signature information is likely to be used.

g. Incident response procedure will have been established. A fully resourced computer incident response team is likely to been stood up. Incident recovery procedures, controlled close down, impact assessment and

recovery procedures will be documented and regularly tested. Incidents are reported to GovCertUK and CINRAS as required.

h. The system design and security documentation is likely to have been subject to independent review by CESG, CLAS Consultants or CTAS approved supplier and appropriates action taken to mitigate any significant issues identified. The service configuration is likely to be subject to regular independent health check by CESG, CHECK approved supplier or a CTAS approved supplier.

Situational Awareness

515. Situational awareness provides the means of obtaining and maintaining awareness of the vulnerabilities of a service, detecting attacks and responding in a timely, coordinated and prioritised way

Level 0 Awareness – no specific measures

516. At Level 0 no special measures need to be taken beyond routine good practice such as keeping up with security patches and attention to firewall and other incident logs.

Requirements

517. No explicit requirements.

Examples

518. Services that might fall into this category are those that provide general information to the public and are in low threat environments. For example, standalone kiosks located in libraries that provide information on local council services.

Provision

519. General awareness of system vulnerabilities and threats would be obtained by monitoring supplier, GovCertUK and other sites.

520. Standard commercial products are likely to be used to provide the system services. Management arrangements are in place to ensure that these devices are patched as required to maintain the secure state.

521. Periodic review of system and other accounting logs is likely to be performed to enable potential incidents to be detected.

Level 1 Awareness – aware

522. At level 1 the service is assessed of being of interest to a class of adversaries but no specific threats have been identified. General awareness of attacks and

potential vulnerabilities of the systems providing the service needs to be maintained.

Requirements

523. At Level 1 a management framework for the monitoring of the service and its vulnerabilities should be established. This includes assigning responsibilities for audit, incident response and reporting to individuals.

524. Proactive monitoring of key servers and boundary protection devices should be performed. Protective monitoring services should be appropriately resourced and integrated with business activities.

525. Accounting logs should be generated on servers and network protection devices. The events record should include as a minimum, all failure events, changes in configuration or security policies and the execution of privileged commands. Accounting logs should:

    a. reveal a unique identification (ID), e.g. the ID of the individual or process performing a function;

    b. reveal the date and time of an event or function or series of related functions;

    c. identify the physical or logical address (or both) where the function took place (this could be a terminal address, boundary device port address or similar);

    d. reveal the type of service being executed.

526. All clocks on all devices that are subject to monitoring should be synchronised.

527. An operational cycle should be established to enable the early detection of potential threats. This should include at least weekly review of accounting logs.

528. Monitoring of relevant commercial bulletin boards should be performed to enable early identification of information of vulnerabilities and to allow timely installation of patches.

529. A longer term reporting cycle should also be established to review trends and enable the identification of areas requiring improvement.

530. A documented set of processes for incident management should exist. These should be tested to ensure their effectiveness. The procedures should cover the incident response plan, incorporating actions that may range from immediate restoration of service to partial restoration or suspension of service. A controlled closedown process should be available, maintaining the provision of essential

business services as far s possible. Following an incident, an Impact assessment should be made of whether any damage, including loss of data integrity, has occurred and a recovery plan drawn up. System security staff should examine all incidents of attack and determine whether any additional security controls should be put in place.

Examples

531. Examples of service that might merit level 1 protection are those that provide general information to the public. Malicious attack, such as defacing of the website might cause minor embarrassment to government and minor inconvenience to the users of the service.

Provision

532. At Level 1 responsibilities are defined and processes documented for monitoring commercial bulletin boards and supplier sites to ensure the early identification of vulnerabilities and the need to install system patches. Responsibilities for system maintenance are defined and processes documented, for patch testing and installation. Audit responsibilities are defined and audit processes are documented.

533. Standard commercial tools are used to meet the requirements. All servers and boundary protection devices are configured to produce accounting logs. Security events to be included in the accounting logs include:

    a. all failure events;

    b. logon and logoff events;

    c. audit events;

    d. the execution of all privileged commands.

534. For all events recorded in the accounting logs the following information as a minimum is recorded:

    a. the unique ID of the individual or process associated with the event

    b. the data and time of the event;

    c. the source of the event (e.g. the physical or logical address (IP header, MAC));

    d. the type service being executed (e.g. service or protocol name and number).

535. Regular monitoring of accounting output is performed to detect potential breaches. This is performed at least weekly. Automatic alerting on critical events is set up to ensure a timely response.

536. System provided activity monitoring tools are regularly used to confirm that the service is operating within acceptable bounds.

537. Accounting logs are archived. Retention periods are determined in accordance with legal and business requirements and are likely to be at least 3 months.

538. Long term trend analysis is performed. Overall policy direction is reviewed and opportunities for improvement identified. This is likely to occur at least annually.

539. The incident response plan has been developed in accordance with ISO 18044 [aa]. The plan is based on being able to perform an initial response to critical events in less than a day and commence a full investigation within 1 week. The plans are subject to at least annual testing to ensure it is effective.

Level 2 Awareness – active awareness and response

540. At Level 2 the service is assessed as being of interest to specific capable adversaries. Active awareness of the security state of the service environment needs to be maintained and a central response team needs to be in place to ensure a coordinated and prioritised response to incidents. Active links to national response centre are likely to be in place to enable early identification of new threats and vulnerabilities and responses to be taken to these.

Requirements

541. All the requirements at Level 1 apply at Level 2. In addition, at level 2:

    a. a full range of information assurance components is expected to be deployed within the environment. This includes boundary protection devices, import and export control devices, intrusion detection and prevention systems. Accounting logs are produced by all IACs and servers. Accounting logs should be reviewed to ensure compliance with the system security policy.

    b. audit data from the different IACs should be consolidated within a central security information management (SIM) system. The SIM should support the automatic correlation and analysis of the accounting data. Commercial attack signature vectors would be expected to be used with the SIM.

    c. active monitoring of supplier web sites, GovCertUK and over source of information on current vulnerabilities is performed. An active link to the national government response centre is maintained to enable early identification of new threats and vulnerabilities.

d. a central incident response team should be established. This should have an agreed set of documented incident response plans to cover all significant eventualities. These incident plans should be regularly tested to ensure that they are effective and current.

e. a forensic readiness plan should be established and frequently tested.

f. all services should be operated in accordance with commercial good practice.

Examples

542. Examples of services that might merit level 2 Awareness protection include:

a. On-line self assessment tax return services;

b. On-line access to medical information or the results of health screening;

c. A client undertakes a financial transaction. Electronic attack might result in disclosure of credit or debit card details, causing significant distress and inconvenience to the client.

Provision

543. Provision is similar to Level 1. This will be supplemented by the use of commercial security products that provide boundary protection, import and export controls and host and network based IDS. These will all provide audit information. Accounting will include recording of:

a. business data importing and exporting at the boundary;

b. suspicious activity at the network boundary;

c. internal workstation, server or device status;

d. suspicious internal network activity;

e. events relating to network connections;

f. session activity by user and servers;

g. data backup status;

h. status of the audit system.

544. Accounting data will be consolidated and analysed within a central security information management system. This will be manned during core business hours. Critical events will be alerted to the response team at all times.

545. Accounting logs will be protected to ensure their integrity. The logs will be archived. Retention periods will be determined from the business needs but are unlikely to be less than 3 months.

546. Accounting logs will be regularly audited (at least once a week).

547. A central incident response team exists to ensure a coordinated and prioritised response to incidents. The team plan to be able to perform initial response to critical events in under 4hrs and to start a detailed investigation within 2 days.

548. An active link with the HMG national response centre will be established to enable early identification of new threats and vulnerabilities and responses to be taken to these.

549. Service monitoring processes are operated and provided in accordance with good practice on service management (for example, ISO/IEC 20000 -1 [bb] and ISO/IEC 20000 -2 [cc]).

550. Analysis and checking for security breaches will be used on a routine basis. Standard commercial tools will be used to perform this

551. Regular review activities of the Information Security Management System and associated processes will be performed to check its effective and to allow continuous improvement.

552. A forensic readiness plan will be in place. This will have been produced in accordance with the good practice guidance and will be regularly tested to ensure its continuing effectiveness. This should be implemented in accordance with CESG Good Practice Guide 18 [dd].

Level 3 Awareness – informed awareness and coordinated response

553. At level 3 the Service is assessed as being of interest to specific capable adversaries with evidence of ongoing activity against the service or its peers.

554. A comprehensive computer network defence capability is deployed at this level with ongoing links to a national threat and incident monitoring service.

Requirements

555. All the requirements at Level 2 apply at Level 3.

556. At Level 3 more comprehensive monitoring of the environment should be performed. This includes scanning the system to identify vulnerabilities and to enable early detection of unauthorised changes in network and system configuration.

557. Event data from all Information Assurance Components (IACs) should be fed back to a central coordination centre that is provided with the tools to allow the consolidation and analysis of the data. The latest government signatures for signs of attack should be used within the analysis tools to identify potential attack.

558. Tools should be provided to enable the response centre to priorities incidents and manage their response.

Examples

559. An example of a service for which Level 3 awareness may be appropriate is a defence e-procurement service, or travel booking service used by the FCO, VIPS or Defence staff.

Provision

560. Provision at Level 3 builds on that at Level 2.

561. A comprehensive fully resourced computer network defence capability will be deployed including:

    a. boundary protection devices;

    b. import/export filtering;

    c. network and host based IDS (host on critical servers), likely to exploit both anomalous behaviour and signature based approaches;

    d. vulnerability scanning;

    e. network discovery (to allow real time audit of network configuration)

    f. network behaviour analysis.

562. Event data from all IACs (including internal devices) will be fed back to a central coordination centre that is provided with tools to allow the consolidation and analysis of this data. Latest government attack signature data will be provided to enable analysis of event information.

563. An active link to the government national response centre will be established to enable early identification of new threats and vulnerabilities and responses to be taken to these.

564. Audit and accounting records will be archived to allow future forensic analysis. Retention periods for archive data will be determined by business needs but are unlikely to be less than 12 months.

Business Logic Components

565. This security component covers the measures necessary to ensure accountability and non-repudiability of a transaction. It is considered under two headings:

    a. Internal accountability – this is concerned with the measures taken to establish the traceability and accountability of significant transaction steps within the server environment.

    b. External accountability – this is concerned with the measures taken to establish the accountable authority for, and provenance of, transfers of data to and from external sources.

Internal accountability

566. The Internal Accountability security component provide the means by which assurance is gained that the transaction logic is correct, that information is not changed in an unauthorised manner when received, stored or processed within the server environment and that the necessary accounting logs are maintained to enable traceability and accountability.

567. Many of the measures required to provide the required internal accountability are common to the measures need to protect the information access and availability of data within the server environment. There is therefore a significant degree of commonality between the Information Access and Information Availability Security Components levels and the Internal Accountability Security Component Levels.

568. The organisational, personnel and physical security requirements of the organisations managing the servers are described in the Organisational Assurance Security Component requirements.

Level 0 Internal – no specific measures

569. At Level 0 there are no explicit internal accountability requirements other than those required to meet commercial practice for financial accounting and asset management.

Requirements

570. Commercial good practice should be followed to minimise the vulnerability of the system to attacks on the integrity of the service provided and the data captured, processed and stored.

571. A means should be provided to enable the detection of any breach in data integrity held within the server environment. This may be a manual process or automated tools may be used.

572. Data archive and data backup should be performed on a regular basis. The frequency of data backup should be determined from the level of data loss the business is prepared to accept.

573. The archive and backup process should be regularly tested to confirm its correct operation. Backup and archive data should be afforded the same level of protection as the operational data to ensure that its integrity is maintained.

Examples

574. Services for which Level 0 internal accountability is appropriate are those for which failure of the transaction is likely to result in minimal inconvenience to any party. For example, a service that provides publicly available information from a government website. Corruption of the information due to a malicious or non-malicious impact would cause at most minimal inconvenience to the client.

Provision

575. At Level 0, commercial products are likely to be used to meet the requirements. The in-built security features of these products are likely to be sufficient to meet the security needs. The products will be configured and hardened in line with commercial good practice. No specific security enhancement will be required to these products. They will be assumed to correctly. Clients may be able to detect where modifications have occurred (e.g. document format errors, incomplete web pages), but the ability to be able to detect modifications is not a high business need.

Level 1 Internal – auditable

576. At Level 1 a basic level of accountability for transactions is required. Standard commercial levels of quality control and testing on transaction logic are required. Basic accounting records are produced and retained in a secure manner that can be used to relate a transaction to an identified individual at a specific time. Standard commercial methods are used to preserve the integrity of records.

Requirements

577. The system should be designed, developed, implemented and operated in accordance with the requirements of Technical Assurance Level 2 or 3. This should include performing independent review of the transaction logic to confirm its validity.

578. Commercial good practice should be followed to minimise the vulnerability of the system to attacks on the integrity of the service provided and the data captured, processed and stored.

579. An information management policy should be produced. This policy should, as a minimum:

    a. specify what information types are covered;

    b. state the policy regarding protective marking;

    c. state the policy regarding identifying the impact of a breach of integrity on different information and identifying information with high impact;

    d. state the policy regarding identifying the impact of a breach of availability on different information and identifying information with high impact;

    e. state the policy with regard to the type of media to be used for storage;

    f. state the policy regarding data file formats and version control;

    g. state the policy regarding relevant information management standards to be complied with;

    h. define the retention periods and disposal policies;

    i. define the responsibilities for information management functions and for ensuring compliance with the policy;

    j. include the results of consultations with appropriate legal and/or regulatory bodies;

    k. defines requirements for auditing relative to particular document types.

580. Procedures should be in place that ensure that the authenticity and integrity of data can be maintained. The procedures should be documented and cover at least capture, indexing, output, transmission, retention, disposal, backup, data migration, maintenance, security, outsourcing, workflow, self modifying files, maintaining accuracy of date and time of an event, quality control and/or time and version control.

581. Regular audits should be performed to confirm compliance with the information management policy. Certificates of compliance should be obtained.

582. Security risk assessments should be performed and regularly reviewed. The risk assessment should explicitly consider the risks to data integrity. Of particular importance are the security measures implemented to control the information storage media, both the live and backup media. Business continuity plans should give explicit consideration as to how the integrity of information is to be maintained during a disaster and recovery from the disaster.

583. Segregation of roles should be considered for key information management roles, including input reconciliation, quality control, data entry, information disposal and information security.

584. As a minimum, the physical, personnel, procedural, access control, user access management, service operation, service continuity, server hardening, import and export controls and audit requirements defined for Information Access Level 2 should be met.

585. Audit trails should be produced. These audit trails should contain sufficient information to be able to demonstrate all necessary historical activities relating to the data whose integrity needs protection.

586. Access to the audit trail should be limited to those with an explicit need. Access to the audit trail should be audited. The audit trail should be managed to ensure it is understandable and to ensure its authenticity and accessibility. It should be sufficiently comprehensive to enable independent review to confirm all changes to protected information. It should be retained for at least the same period as that of the data it relates. It should include date and time stamp information for each event recorded.

587. For critical records, consideration should be given to the use of cryptographic controls to improve security and provide tamper evidence. Where cryptographic techniques are exploited, key material should be managed in accordance with Business Logic External Accountability Level 2.

588. Where data compression is to be used (e.g. prior to electronic communication) the type of data compression to be used should be carefully considered and assessed for its impact on data integrity.

589. For information that may be stored for a considerable length of time (longer than the lifetime of the current technology) a data file migration strategy should be developed. Records should be kept to demonstrate that integrity has not been compromised in the process of migrating and converting data.

Examples

590. Example transactions that might merit level 1 Internal accountability include:

591. A self assessment tax application for which the client may subsequently seek to deny responsibility for the contents of the return claim forgery or interference or for which incorrect operation of the software could result in invalid financial calculations leading to significant loss or damage to reputation.

592. A service that allows a client to pay a fixed penalty fine. Delay in payment of the fine results in additional penalty charges being incurred.

Provision

593. Standard commercial products are likely to be exploited. These will be configured so that:

a. data is recorded on to final data storage as soon as possible after the time of data capture.

b. access controls are in place to limit those users with write or modify privileges to records to a minimum.

c. anti-virus and other systems used to prevent malicious alteration of stored data files are implemented;

d. backup power supplies or UPS are used to minimise the risk of data corruption in the event of a power failure.

e. full data backup is performed with comparison of backup data to the relevant operational data to confirm its integrity. The frequency will be determined from the level of data loss the business is prepared to accept. The archive and backup process will be regularly tested to confirm its correct operation. Backup and archive data will be afforded appropriate protection to ensure that its integrity is maintained.

f. checksums or digital signatures may be used to confirm integrity of a stored or transmitted data records and, where appropriate, the identity of the party who originated the data. Procedures will be in place for the verification of signatures and for recording verification timings. Where automated controls to detect alterations to or removal of data do not exist, manual random checks to verify that critical records which have been frozen have not been altered or removed will be performed on a regular basis.

g. lossless techniques are used for data compression where any reduction in detail is not acceptable;

h. automatic processes are in place to verify the receipt of electronic communications. For example, if SOAP is used for web transactions it will be configured to require receipts to be generated by the receiving system.

i. accounting logs will be produced that enable a full record of the changes made to a record. For compound documents audit trails will be such that the historical content of the data file can be assessed at any relevant time

j. WORM technology may be used for data storage of critical records for which it is important to prevent the modification of stored records.

k. import and export controls are likely to be based on blacklisting. Procedural controls are likely to be used to control the import and export of objects from media (e.g. CDs). Mail and other electronic imports are likely to be screened automatically at the gateway to the system. Dangerous file types (e.g. executables) are likely to be automatically blocked or quarantined at the gateway. The list of file types to be blocked or quarantined is likely to be based on a blacklisting approach. Data that is likely to be reasonably required by the business will be allowed by default.

l. the communications across the gateway will be minimised to those that are reasonably required by the business. Filtering technology is likely to be used to remove SPAM, SPIT and SPIM. All import and exported objects will be subject to anti-virus scanning using a commercial anti-virus product. An anti-virus strategy will be in place to ensure the timely update of anti-virus signatures.

m. standard system provided activity monitors are likely to be used to regularly confirm that the system is operating in accordance with its expected parameters and to enable any suspicious activity or patterns of activity to be identified. Standard system-provided accounting logs will be reviewed by appointed security personnel for the system to ascertain whether there is any activity or pattern of activity that might indicate an unexpected electronic attack on the system. Account logs are likely to be reviewed at least monthly. Alerts are likely to be configured for critical events to ensure a timely response. Accounting logs will be retained to enable a record of transaction times and record changes. Access to the logs will be strictly controlled to minimise the risk of tampering.

Level 2 Internal – Accountable

594. At Level 2 strong measures are needed to ensure that those involved in a transaction can be held to be account. At this level it is anticipated that it may be necessary to present evidence in support of legal action.

Requirements

595. The system should be designed, developed, implemented and operated in accordance with the requirements of Organisational and Technical Assurance Level 3. This should include performing independent review of the transaction logic to confirm its validity.

596. The requirements of Level 1 should be satisfied. The measures required should however be stronger and it should be possible to demonstrate that all relevant requirements of BSI BIP 0008-1 [ee], BIP 0008-2 [ff] and BIP 0008-3 [gg] are satisfied.

597. Government good practice should be followed to minimise the vulnerability of the system to attacks on the integrity of the service provided and the data captured, processed and stored.

Examples

598. Level 2 internal accountability applies where it is necessary to be able to hold a person accountable for a transaction. For example, passport issuing services may need Level 2 accountability as part of the measures necessary to prevent the fraudulent issue of passport. Driving licence record services may need Level 2 accountability as part of the measures necessary to prevent the fraudulent issue of licences or the fraudulent modification of driving licence endorsements.

Provision

599. Provision of the services at Level 2 is similar to that at Level 1. The main areas of difference are that:

    a. The technical controls will be supplemented by strong physical, procedural and personnel security measures to ensure the required authenticity, accountability and integrity of data can be maintained.

    b. All personnel with physical access to the system are likely to have been vetted in accordance with BS requirements. Personnel with more privileged access, for example system administrators, are likely to have been subject to SC vetting or equivalent.

    c. The physical controls protecting the environment in which servers, backup media, etc are stored will be sufficient to deter a skilled attacker.

    d. Level 2 or Level 3 situational awareness is likely to have been implemented.

    e. Regular audits of all accounting records will be performed.

    f. Regular independent inspections will be performed to confirm conformance with the security procedures.

    g. Products providing key elements of the security enforcing functionality are likely to have been subject to independent assurance. The products are likely to have achieved at least EAL 3 accreditation under Common Criteria [s]. Cryptographic products are likely to have been subject to certification to Baseline grade by CESG. Other products for which Common Criteria or CAPS approval [hh] is inappropriate are likely to have been subject to CCT Mark testing.

h. The system design and security documentation is likely to have been subject to independent review by CESG, CLAS Consultants or CTAS approved supplier and appropriate action taken to mitigate any significant issues identified. The service configuration is likely to be subject to regular independent health checks by CESG, a CHECK approved supplier or a CTAS approved supplier. This will be at least annually and after any significant configuration change.

External accountability

600. The external accountability security component covers the measures taken to establish the accountable authority for, and provenance of, transfers of data to and from external sources.

601. Three levels of external accountability are defined.

Level 0 External – no specific measures

602. At Level 0 items received are taken at face value.

Requirements

603. There are no explicit external accountability requirements though any system logs may be used to establish a transaction history if needed.

Examples

604. Services for which Level 0 external accountability is appropriate are those for which failure of the transaction is likely to result in minimal inconvenience to any party. For example, a service that provides publicly available information from a government website. Corruption of the information due to a malicious or non-malicious impact would cause at most minimal inconvenience to the client.

Provision

605. At this level items received or transmitted are taken at face value. Normal service elements provide sufficient assurance that an object originated from a particular source. For example, an e-mail from user@isp.net.uk would be sufficient to assume the information provided is from user. A web page http://www.dept.gov.uk/ would be sufficient to confirm the information it contains is from dept. No special mechanisms are implemented to support traceability. The risks associated with impersonation are acceptable to the business at this level.

606. Normal service components would be used to confirm that a transaction has occurred. For example, a confirmation e-mail provides sufficient evidence that the transaction was completed by the government service.

Level 1 External – auditable

607. Level 1 provides a basic level of accountability for transactions performed. Evidence of receipt of a transaction is provided by the service to the client. It would be relevant for transactions of an official nature in which failure to complete the transaction may be interpreted as a statutory infringement that may incur a penalty, or which may have a significant impact on a third party. A strong and persistent binding between the transaction and the security information, while desirable, is not essential and other means of providing the required traceability and accountability can be exploited.

Requirements

608. Level 1 Internal Accountability requirements should be met.

609. A transaction should:

    a. occur via a trusted route that provides basic assurance as to the identity of the originator and receiver (where relevant); or

    b. a trusted out of band route should be used to confirm the transaction with the originator before transaction completion; or

    c. a digest of the transaction (or the transaction) should be signed by the originator to provide evidence of origin and to provide integrity protection.

610. If signatures are used they should be verified by the recipient of the transaction, or by a third party. Ownership of any public keys should be verified by a recognised entity, which may be the recipient or some other party. Verification should include checking that the end certificate and all those in the required trust path have not been revoked. It should also include checking all certificates have been issued under an appropriate policy for which they are being relied on. Both the PKI service provider and business service provider should synchronise their time with a reputable time source.

611. Accounting logs should be generated and kept, showing transaction times and records of system operation. Sufficient information should be recorded within the accounting logs so that it can be demonstrated to a third party (if needed) who the transaction originator was. A response demonstrating receipt of a transaction should be returned to the transaction originator (whether the transaction is successful or not).

612. Evidence of receipt of a successful transaction should be provided by the service. The receipt should confirm the success of the transaction.

613. The integrity and authenticity of the returned response should be protected at a comparable level to the original transaction. It should contain sufficient

information that the recipient is able to validate the transaction against what they submitted.

615. Retention periods for accounting logs and other transaction periods should be determined as part of the design process.

616. Any requirements for the clients of a service to retain records should be clearly communicated to them.

Examples

617. Examples of services for which level 1 External Accountability include:

a. Payment for a low value goods and service that are delivered to the recipient's known address;

b. Payment of a fixed penalty fine for which the Government could deny receipt incurring additional penalty charges and loss for the client;

Provision

618. At this level a transaction could occur via a trusted route that provides basic assurance as to the identity of the originator and receiver (if relevant) of the transaction. For example, it might involve the use of TLS with Server and Client Authentication.

619. Basic accounting records would be produced and retained in a secure manner that can be used to relate a transaction to an identified client at a specific time and provide information on success or failure of the transaction.

620. Additional degrees of trust may be achieved by the use of informal measures to deter later repudiation of a transaction. For example, the client is provided at intervals with a list of recent transactions. It is important that expert guidance be sought when setting up such schemes, as the additional trust achieved is often illusory unless the scheme is carefully constructed. Such schemes are rarely foolproof, it is therefore important that the limits of such schemes are understood and accepted by both parties to the transaction. However, these methods may provide a useful extra degree of trust in specific cases and provide the client with greater confidence.

Level 2 External – accountable

621. This level would cover transactions of an official nature in which failure to complete the transaction might have a substantial financial impact (which might not be recoverable), or impact on the health or safety of installations or individuals. Such transactions may be attractive to criminal exploitation leading to a substantial risk of fraud or criminal damage. At this level there is a need for strong and persistent binding between transaction and security information.

Requirements

622. Level 2 Internal Accountability requirements should be satisfied.

623. A transaction or a digest of the transaction, signed by the originator, should be used to provide evidence of origin and to provide integrity protection to the transaction details.

624. The signature should be verified by the recipient of the transaction, or by a third party. Ownership of any public keys should be verified by a recognised entity, which may be the recipient or some other party. Verification should include checking that the certificate has not be revoked or suspended and that it has been issued under an appropriate policy. Time should be synchronised between the PKI service provider and the business service provider.

625. Accounting logs should be generated and kept, showing transaction times and records of system operation.

626. The signing algorithm used should be selected to be compliant with HMG IA Standard 4. Private keys used for signing should be protected using recognised, cryptographically assessed and approved software or hardware tokens. Trust anchors should be distributed to where they are used by a secure means that enables their origin to be validated and confirmation that they have not been tampered within in transit confirmed. The trust anchors should be stored in a secure environment that provides tamper protection.

627. The PKI services used should have been approved under tScheme [ii] or an equivalent.

628. A response demonstrating receipt of a transaction should be returned to the transaction originator (whether the transaction is successful or not).

629. It should confirm success or failure of the transaction.

630. The integrity and authenticity of the returned response should be protected at a comparable level to the original transaction.

631. The receipt should be signed by the originator.

632. It should contain sufficient information that the recipient is able to validate the transaction against what they submitted.

633. Retention periods for accounting logs and other transaction periods should be determined as part of the design process.

634. Any requirements for the clients of a service to retain records should be clearly communicated to them.

Example

635. Example transactions that might merit level 2 external accountability include:

a. An organisation files a fraudulent tax return electronically and, upon being challenged, may deny submitting the return.

b. A client receives results of medical testing electronically. The client needs to be assured that the results are indeed from the service provider and could not have been altered in transit.

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

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

Provision

636. At Level 2 it is expected that commercial PKI technology will be exploited. The technology used would have undergone independent assurance by a recognised organisation to confirm that it provides adequate security functionality (e.g. obtained certification at EAL 3 or 4 under the Common Criteria scheme). The cryptographic modules used would have been expected to have been validated by CESG or a FIPS 140 accredited laboratory.

637. The PKI services would have validated against HMG requirements to confirm they have been implemented as expected. This could involve, for example, obtaining tScheme accreditation.

638. Private keys used to sign the transactions are expected to be generated and stored within a secure environment. It is likely that evaluated Smart Cards will be used to provide this secure environment.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 5 - Assurance Components

Key Principles

- Covers the activities required to confirm the secure end-to-end delivery of a service.
- Includes the design review, implementation, configuration, operation and disposal from a security viewpoint.
- Considers Organisational Assurance covering management, procedural, personnel and physical security aspects of the service delivery against security requirements.
- Considers Technical Assurance covering design, implementation, configuration, maintenance and operation of the e-government service against security requirements.

Introduction

639. Assurance components covers the activities required to confirm the secure end-to-end delivery of a service. It covers the review of the design, implementation, configuration, operation and disposal activities to ensure that the security requirements are met. Two aspects are considered:

    a. Organisational Assurance;

    b. Technical Assurance.

Organisational Assurance

640. Organisational assurance covers the review of the organisations involved in the delivery of a service to ensure that the required management, procedural personnel and physical security arrangements are in place to secure the service.

Level 0 Organisation – no specific measures

Requirements

641. There are no explicit requirements for external independent audit of the organisation's information security management system. Self certification is expected to provide sufficient assurance that the organisation is effectively managing its security.

Examples

642. An example of a service that falls into this category is the provision of a public website that provides general publicly available information. A breach in the security would be expected to have a minimal impact.

Provision

643. While there are no formal requirements for independent external assurance to be obtained of the effectiveness of the organisation‘s information security management system, the service provided by the organisation is still expected to be designed, implemented, configured, operated and maintained in accordance with commercial good practice.

644. The organisation is expected to have a documented information security management system. This information security management system (ISMS) is expected to meet the requirements of ISO/IEC 27001 [jj] although independent certification of this is not required at this level. An information risk policy is expected to have been defined. This policy is expected to clearly document the organisations risk appetite. A process for identifying Information risks and allocating these to appropriate owners and managers is expected to have been defined and be in operation. In assessing risks, consideration of those risks that arise from the supply chain are expected to be considered.

645. Management arrangements for information security are expected to have been established. This is expected to include senior leadership. Processes are expected to be in place to enable the organisation to confirm its compliance to the ISMS. Periodic internal audit of compliance is expected to be performed to reassure the organisation’s Board that security is being effectively managed.

646. The organisation is expected to have effective personnel security controls in place. This includes ensuring security role and responsibilities are defined and documented in relevant contracts. Pre-employment screening is expected to verify individuals’ identities and the claims they make in their application. CPNI guidance on pre-employment screening is provided in [kk]. Once employed, a programme of training, education and security awareness is expected to be provided. On termination or change of employment processes to ensure the return of assets, removal of access rights and ensure individuals are aware of their ongoing security obligations are expected to be in place.

647. Physical Security controls are expected to be in place to prevent unauthorised physical access, damage and interference to the organisation’s premises and information resources. CPNI guidance on physical security controls is provided in [ll].

648. The organisation is expected to have a document incident management plan – ISO/IEC 18044 [aa] provides good practice guidance.

649. An assessment of the organisation IA maturity against the CESG IA Maturity Model [mm] is expected to achieve at least level 1.

650. The design, implementation and operation of the service is expected to be performed in accordance with good practice (e.g. in accordance with the service management requirements of ITIL [nn]. Formal configuration and change control procedures are expected to be in place. Changes to an element of the service are expected to be subject to acceptance testing within a test environment prior to implementation in the operational environment. Formal sign-off of a change by the service manager is expected to be obtained before the changes are made within the operational environment.

651. Other standards relevant to the design, implementation and operation of the service include:

    a. ISO 9000 and ISO 9001 for quality assurance;

    b. ISO 20000 for service management;

    c. BS25999 for disaster recovery;

    d. BS25999 and ISO 24762 for business continuity planning.

652. Independent certification of compliance with the standards would not however be expected.

Level 1 Organisation – independent assessment

Requirements

653. Independent assurance is required that those involved in the provision of the service and the locations from which they provide the service have appropriate (commercial good practice) organisational, physical and personnel controls in place. This includes assurance that:

    a. the organisation's Information Security Management System is compliant with ISO 27001 or an equivalent standard;

    b. the organisation has an effective process for assessing and managing the risk associated with personnel;

    c. the organisation has effective physical security measures in place that are capable of deterring a skilled attacker;

    d. an assessment of the organisations IA maturity against the CESG IA maturity Model [mm] is at least level 2;

    e. relevant service design, implementation and operation standards (e.g. ISO 9000) from a UKAS accredited certification organisation.

Example

654. Example services for which level 1 organisational insurance is relevant include:

    a. A service that enables a client to purchase a low cost government publication over the Internet. The impact of failure is inconvenience and possibly recovering or refunding incorrect payments.

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

Provision

655. The organisation is expected to have an information security management system in place that is compliant with ISO 27001 or equivalent standard. Effective security governance arrangements are expected to have been established. This includes a board level senior information risk owner who:

    a. Is accountable;

    b. Fosters a culture for protecting and using data;

    c. Provides a focal point for managing information risks and incidents;

    d. Is concerned with the management of all information assets.

656. The SIRO is expected to be supported by an Accreditor who:

    a. provides policy guidance to staff;

    b. ensures ICT systems have accurate risk assessments in compliance with national and organisational policy

    c. audits all the security aspects of the service provider's implementation of appropriately assured technical and non-technical countermeasures, including reviewing all security-relevant documentation.

    d. formally accredits ICT systems on behalf of the SIRO/board;

    e. reaccredits ICT systems as required.

657. Personnel with potential access to the information assets are expected to be subject to background checks. This includes checks on their identity and on their employment, academic and professional qualifications. References are expected to be checked by following up in writing with written evidence of all

qualifications. Staff performing key management and security roles are likely to have at least three years' service with the organisation. All personnel with access to information assets are expected to have been required to sign appropriate confidentiality agreements. This agreement should expressly prohibit the unauthorised disclosure or amendment of information and should make clear the penalties if such incidents occur. Management responsibilities for security are expected to be defined. Formal disciplinary process is expected to be in place for dealing with employees who have committed a security breach. Staff duties are likely to be rotated in order to avoid dependency on key individuals and to allow any unauthorised activities to be identified by changing roles. Security awareness, education and training is provided to all staff including providing regular updates. Responsibilities for performing employment termination or change of employment activities are clearly defined. Procedures are in place to ensure all assets are returned when no longer needed and to cover the revocation of access rights. Good practice guidance on managing the risks associated with personnel may be found on the CPNI website [oo]

658. Physical security controls that are adequately resistant to unauthorised access are expected to have been implemented. The CPNI website provides guidance on identifying appropriate physical security controls [ll]. The controls are likely to include segregated secure areas for accommodating information assets of particular sensitivity and to which only staff that have undergone an appropriate level of security checking would have access. Measures to manage the risk of computer screens or other documentation being overlooked by possible attackers are expected to have been implemented. Physical intrusion detection systems and access control systems are expected to be present, event information will be recorded and monitored. Access control systems uniquely identify every person entering the location. Security passes are expected to be issued to and worn by all authorised personnel with access to the location. There are likely to be frequent security guard patrols. Rigorous supervision of building and maintenance works is performed. Restrictions on staff carrying specified personal items, such as PDAs, USB and other storage devices, mobile telephones and cameras in sensitive areas are likely to be in place. Controls over the removal of assets from the location, including paper records and removable media are also in place. CCTV monitoring of sensitive areas as well as building entrances, exits, vulnerable points and perimeter is likely to be in place.

659. Audit of the ISMS, personnel and physical controls may be performed by a UKAS accredited ISO 27001 auditor.

Level 2 Organisation – government approved assessment

Requirements

660. Independent assurance is required that those involved in the provision of the service and the locations from which they provide the service have appropriate

(commercial good practice) organisational, physical and personnel controls in place. This includes assurance that:

a. An Information Security Management System is in place that meets the requirements of Security Policy Framework (SPF) [[a]].

b. Personnel controls are in places that meet the requirements of SPF Security Policy Number 3. Staff in privileged positions (e.g. system administrators) are likely to have at least SC clearances. Other staff are likely to have at least BS clearance.

c. Physical controls are in place that meets the requirements of SPF Security Policy Number 5.

d. An assessment of the organisations IA maturity against the CESG IA Maturity Model [[a]] is at least level 3;

e. Relevant service design, implementation and operation standards (e.g. ISO 9000) from a UKAS accredited certification organisation.

Example

661. Example services for which level 2 organisational assurance is appropriate include:

a. Electronic filing of income tax and Value Added Tax (VAT) returns;

b. Services that give access to sensitive private information, for example a person's medical record.

Provision

662. The organisation's information security management system is expected to be compliant with the Security Policy Framework.

663. All personnel with potential access to the service assets are expected to have been cleared in accordance with the Baseline Personnel Security Standard. Higher levels of security vetting may be required for some key personnel (e.g. those with System Administrator privileges). Appropriate aftercare is expected to be provided.

664. The physical controls in place at the locations at which the service assets are located will have meet the requirements stipulated in SPF Security Policy Number 5 for the storage and process of information with a protective marking of at least Restricted. Higher levels of controls may be required for some services.

665. Assurance that the organisation meets the required standard is expected to be obtained through audits performed by Defence Security Standards Organisation, CESG, the relevant Departmental Security Officer or another organisation approved by the Departmental Security Officer.

666. Certification of compliance with ISO standards is expected to be provided by a UKAS accredited organisation.

Technical Assurance

667. The Technical Assurance security component covers the technical review of the totality of an e-government service to ensure that it is designed, implemented, configured, maintained and operated in accordance with the security requirements.

Level 0 Technical Assurance – no statement

Requirements

668. There is no requirement for assurance that the security requirements are met by the service.

Examples

669. An example of a service that falls into this category is the provision of a public website that provides general publicly available information for which a breach in the security of the service is expected to have a minimal impact.

Provision

670. While formal independent security assurance that the security requirements are met by the service is not required, a systematic approach to the design, implementation, configuration, maintenance, operation and disposal is expected to be adopted. The key stage in the development of a service and security expected at each stage are as follows:

    a. Service concept development, as part of service concept development a security concept is expected to be produced describing the e-Government service, the top-level threats and the likely nature of the countermeasures;

    b. Service requirements specification and review of compliance. During this stage it is expected that the following security activities will be performed:

        i. analyse the threats and vulnerabilities to the system and produce a risk assessment;

        ii. produce an outline risk management and accreditation document set.

    c. Service design, implementation and test. During this stage it is expected that

i. a structured design techniques is used;

ii. the risks are addressed by appropriated countermeasures;

iii. the security countermeasures are documented in the security design document;

iv. the architecture is locked down to cover only required services, in line with good commercial practice; this is expected to be documented in the security design document;

v. comprehensive functional and non-functional testing of the business application(s) and the systems that host them to confirm their correct implementation.

vi. the system configuration is checked to be compliant with the risk management and accreditation document set;

vii. the residual risk are assessed and either accepted or additional countermeasures identified until the risks are acceptable;

viii. strong audit and accounting measures are implemented;

ix. security operating procedures are established;

d. Service acceptance, including security accreditation. During this stage it is expected that the security countermeasures are tested and reviewed to ensure they meet the requirements;

e. Service delivery. During this stage:

i. the service is operated in accordance with the security operating procedures, including regularly monitoring system logs;

ii. the assurance status of the services is reviewed on a periodic basis to confirm the effectiveness of the countermeasures and security operating procedures and ensure any necessary enhancements are identified;

f. Service close down. During this stage it is necessary to ensure that information assets are removed and transferred to a successor service, if appropriate, destroyed or stored securely in accordance with the service specific security policy.

671. At this level the service delivery manager produces the risk management and accreditation document set including performing the risk assessment and identifying the appropriate countermeasures are identified. The Accreditor is expected to accept these at face value.

672. Key security enforcing functionality would be expected to be provided by good commercial products. These products would not however be expected to have undergone formal assurance.

Level 1 Technical Assurance – independent assessment

673. At Level 1 there is a requirement to obtain independent assurance that the service is operated in accordance with good practice.

Requirements

674. The measures identified at level 0 are to be covered. In addition, at level 1:

a. a formal system development cycle is to be followed.

b. security enforcing functionality used by the service is required to be provided by appropriately evaluated products.

c. a quality review of the service implementation is expected to be carried out by independent policy auditor[5] prior to the service going live, after any major changes, and periodically during its life.

d. verification of the implementation carried out by independent compliance auditors[6] prior to service go live. During the in-service phase, after any significant change to the service and periodic (normally yearly) during its life reverification of the system is expected.

Examples

675. Example of a service that falls into this level include:

a. on-line purchase of low cost government publications;

b. on-line purchase of vehicle tax disks.

Provision

676. At this level a formal system development lifecycle is expected to be followed. Sign off of all element of development is expected before they go into production.

677. A clear documented design that has been subject to rigorous peer review is expected to have been produced.

---

5 One possibility is the use of CLAS consultants.

6 Through the use of, for example, CHECK, CREST or TIGER consultants.

678. Software coding standards are expected to have been developed and implemented to ensure consistent and secure code is developed. The code is expected to be documented and reviewed to support validation. Code review is likely to include review by independent third parties. A Gold Build State of software developed and off-the shelf software that is used is expected to be established. Module level, system-level and overall testing of the software is expected to be performed. This is expected to include final user acceptance testing that would include confirmation that security needs are met. Security testing is expected to include penetration testing (including at the application level). Measures are expected to be in place to ensure the integrity of built system components is maintained while awaiting deployment.

679. Formal configuration and change management procedures are expected to be in place. Configuration control is audited and monitored and all changes documented. Any changes to the system are subject to acceptance testing within a reference facility environment prior to implementation in the operating environment. Formal sign-off of a change by the design authority will occur before the changes are made within the operational environment.

680. All hardware and software used for security critical roles will be purchased from trusted sources (i.e. whose security interests are aligned with those of the stakeholders). If trusted sources cannot be used, specific steps will have been taken to gain assurance that hardware and software products can be trusted.

681. Products providing security enforcing functionality that the service relies on are expected to have been subject to some level of independent assurance. This could involve using products evaluate under, for example CCT Mark, Common Criteria (EAL1-2) and/or FIPS.

682. Appropriately accredited independent security experts (e.g. CLAS consultants) assess the security architecture to confirm that it meets the security requirements. CTAS, CREST, TIGER or CHECK approved suppliers might perform the security compliance audits.

Level 2 Technical Assurance – government approved assessment

Requirements

683. The requirements at level 2 are similar to those at level 1 excepted that:

a. key security enforcing functionality used by the service is required to be provided by appropriately government approved or higher assurance evaluated commercial products

b. policy and compliance audits is required to be performed by CESG approved auditors.

Examples

684. Example services for which level 2 organisational assurance is appropriate include:

a. electronic filing of income tax and Value Added Tax (VAT) returns;

b. services that give access to sensitive private information, for example a person's medical record.

Provision

685. Provision at level 2 will be similar to level 1 accept that:

a. it would be expected that CTAS, CLAS or CESG are used to validate the overall system design. CESG or a CHECK green light accredited organisation is expected to be used to perform a comprehensive health check of the overall service (unless this has been performed by a CTAS organisation [a]).

b. components used within the system are likely to be standard commercial products. Products providing security enforcing functionality that the service relies on will have been subject to independent assurance. Where appropriate this will involve use of products that have been evaluated under Common Criteria to at least EAL 2-3 or CAPS. Other products for which Common Criteria evaluation is inappropriate (e.g. anti-virus, content filtering software) will have been subject to CCT Mark testing.

THIS PAGE IS INTENTIONALLY LEFT BLANK

References

[a] ‘e-Government strategy framework policy and guidelines, registration and authentication’, Office of the E-Envoy, 2002
‘e-Government strategy framework policy and guidelines, trust service’, Office of the E-Envoy, 2002.
‘e-Government strategy framework policy and guidelines, business services’, Office of the E-Envoy, 2002.
‘e-Government strategy framework policy and guidelines, network defence’, Office of the E-Envoy, 2002
‘e-Government strategy framework policy and guidelines, assurance’, Office of the E-Envoy, 2002

[b] ‘Requirement for the Secure Delivery of Online Public Services’ – Part 1 Principles’, CESG, December 2009. Available from the CESG IA Policy Portfolio.

[c] ‘CESG Information Assurance Memorandum 26 – Passwords for identification and authentication’, CESG, Issue 4.0, February 2008

[d] ‘Level 2, Remote Authentication’, IMSPG(02) 05, 2008.

[e] ‘CESG Infosec Memorandum 28 – Performance and Assurance Standards for Biometric Systems Contributing to multi-element identification and authentication’, CESG, Issue 1.0, January 2005.

[f] See for example http://www.cesg.gov.uk/publications/biometrics.shtml

[g] ‘Privacy Impact Assessment Handbook’, Version 2, Information Commissioners Office.

[h] ‘Privacy Engineering’, S Marsh, I Brown, M Khaki, Cybersecurity KTN, 2008.

[i] See the Hannigan reports at
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

[j] 'HMG IA Standard No. 6: Protecting Personal Data and Managing Information Risk’, Issue 1.2, March 2009.

[k] ‘HMG Security Policy Framework, Roles and Responsibilities’, V3.1, November 2009.

[l] ‘Good Practice Guide 6 - Outsourcing and Offshoring: Managing the Security Risks’, CESG, Issue 2.0, October 2009.

[m] `Clinical Systems Security -- Implementing the BMA Policy and Guidelines', A Hassey, M Wells.
see also ‘Security Engineering, R Anderson, Second Edition, Wiley, 2008.

[n] ‘Implementing access controls to protect the confidentiality of patient information in clinical information systems in the acute hospital, I Denley, S Weston-Smith, Health Informatics Journal v 4, December 2008.
‘Privacy in Clinical information systems in secondary care’ British Medical Journal’, I Denley, S Weston-Smith, May 1999.
see also ‘Security Engineering, R Anderson, Second Edition, Wiley, 2008.

[o] See for example
http://www.connectingforhealth.nhs.uk/systemsandservices/scr/staff/impguidpm/ig.

[p] Security Compliance Management Toolkit, available at:
http://technet.microsoft.com/en-us/library/cc677002.aspx

[q] ‘HMG IA Standard 1 – Technical Risk Assessment’, Issue 3.5, October 2009.

[r] ‘HMG IA Standard 2 – Risk Management and accreditation of systems’, Issue 3.2, January 2010.

[s] Common criteria for information technology security evaluation, available at:

http://www.commoncriteriaportal.org/.

[t] See for example http://www.cctmark.gov.uk/

[u] See for example
http://www.cesg.gov.uk/products_services/iacs/check/index.shtml

[v] See for example http://www.crest-approved.org/

[w] ‘HMG IA Standard 4 – Communications Security and Cryptography’, Issue 4.0, October 2009.

[x] ‘HMG IA Standard 5 - Secure Sanitisation of Protectively Marked or Sensitive Information’, Issue 3.1, October 2009.

[y] CESG ‘Good Practice Guide 13 – Protective Monitoring for HMG ICT Systems’, Issue 1.3, October 2009.

[z] See for example
http://www.cesg.gov.uk/products_services/iacs/ctas/index.shtml

[aa] 'ISO/IEC TR 18044 - Information technology -- Security techniques -- Information security incident management', International Organisation for Standardisation, 2004.

[bb] 'ISO/IEC 20000 -1 Information Technology Service Management, Part 1 Specification', International Organisation for Standardisation, 2005.

[cc] 'ISO/IEC 20000-2 Information Technology Service Management, Part 2 Code of Practice', International Organisation for Standardisation, 2005.

[dd] CESG 'Good Practice Guide 18 - Forensic Readiness', CESG, Issue 1.0, October 2009.

[ee] 'BIP 0008-1 -Evidential Weight and Legal Admissibility of Information Stored Electronically. Code of Practice for the Implementation of BS 10008', BSI, 2008.

[ff] 'BIP 0008-2 - Evidential Weight and Legal Admissibility of Information Transferred Electronically. Code of Practice for the Implementation of BS 10008, BSI, 2008.

[gg] 'BIP 0008-3 - Evidential Weight and Legal Admissibility of Linking Electronic Identity to Documents. Code of Practice for the Implementation of BS 10008, BSI, 2008.

[hh] See for example http://www.cesg.gov.uk/products_services/iacs/caps/index.shtml

[ii] See http://www.tscheme.org/

[jj] 'ISO/IEC 27001 – Information technology -- Security techniques -- Information security management systems – Requirements', International Organisation for Standardisation, 2005.

[kk] 'A good practice guide on pre employment screening', CPNI, 2nd Edition.

[ll] See http://www.cpni.gov.uk/ProtectingYourAssets/physicalSecurity264.aspx

[mm] HMG Information Assurance Maturity Model and Assessment Criteria', CESG and Cabinet Office, V3.0 2009.

[nn] IT Infrastructure Library, see for example http://www.itil-officialsite.com/home/home.asp

[oo] www.cpni.gov.uk

[pp] 'HMG Security Policy Framework', Cabinet Office, V3.0, November 2009.

Glossary

BMA	British Medical Association
CCT Mark	CESG Claims Test Mark
CCTV	Closed Circuit Television
CPNI	Centre for Protection of National Infrastructure
CTAS	CESG Tailored Assurance Scheme
DoS	Denial of Service
DVLA	Driver and Vehicle Licensing Agency
EAL	Evaluation Assurance Level
e-GSF	e-Government Security Framework
FCO	Foreign and Commonwealth Office
FIPS	Federal Information Processing Standard
GPG	Good Practice Guide
IA	Information Assurance
IAC	Information Assurance Component
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
IPS	Identity and Passport Service
ITIL	Information Technology Infrastructure Library
NHS	National Health Service
NIAS	National IA Strategy
NTP	Network Time Protocol
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement
SPIM	Spam over Instant Messaging
SPIT	Spam over IP Telephony
SSL	Secure Sockets Layer
VPN	Virtual Private Network

Customer Feedback

CESG Information Assurance Guidance and Standards welcomes feedback and encourage readers to inform CESG of their experiences, good or bad in this document. We would especially like to know about any inconsistencies and ambiguities. Please use this page to send your comments to:

Customer Support
CESG
A2j
Hubble Road
Cheltenham GL51 0EX
(for the attention of IA Policy Development Team)

Fax: (01242) 709193 (for UNCLASSIFIED FAXES ONLY)
Email: enquiries@cesg.gsi.gov.uk

For additional hard copies of this document and general queries please contact CESG enquiries at the address above

PLEASE PRINT

Your Name:

Department/Company Name and Address:

Phone number:
Email address:

Comments:

THIS PAGE IS INTENTIONALLY LEFT BLANK

IA
CESG
B2h
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Fax: +44 (0)1242 709193
Email: enquiries@cesg.gsi.gov.uk