VANguard Certification Practice Statement (CPS)

1 Introduction

1. The Department of Industry and Science, hereafter referred to as the 'Department', is responsible for managing the VANguard Program.

2. The VANguard Program is a whole-of-government initiative that aims to provide value added services around a Validation Authority to government agencies (Australian, State, Territory and Local governments).

3. The VANguard Program uses a Public Key Infrastructure (PKI) to:
   - test and verify an assertion so that the receiver of a digital message can be confident of both the identity of the sender and the integrity of the message
   - provide independent and indisputable evidence of online business-to-government transactions ensuring non-repudiation (time stamping services).

4. The VANguard Program uses a PKI with a Root Certificate Authority (RCA), and two subordinate CAs – the Organisational CA (OCA), and the Notary CA.

5. The RCA issues the OCA and the Notary CA. The OCA and the Notary CA issue the VANguard system certificates, as well as issue certificates to Agencies that subscribe to VANguard services.

6. VANguard also issues copies of the VANguard system's public certificates to relying parties.

7. Certificate services, including CA management and operations for VANguard, are provided using the Symantec Gatekeeper accredited Managed Public Key Infrastructure (MPKI).

1.1 Overview

8. This document, the VANguard Certification Practice Statement (CPS), outlines the policy and operational matters for the VANguard PKI, including the practices that Symantec uses in issuing, revoking, and managing VANguard certificates.

9. This CPS should be read in conjunction with the relevant Certificate Policy (CP) document and PKI Disclosure Statement (PDS), which set out the rules regarding the applicability of a certificate to a particular Agency, and contains information about the specific structure of the relevant certificate type.

10. The VANguard PKI provides Certificate Authority (CA) and Registration Authority (RA) services under this CPS and relevant CP and PDS.

11. The obligations of the VANguard PKI entities are also set out in the relevant CP, as well as other documentation, that includes:
    - the relevant PDS that provides additional detail and further provisions that apply to the CPS for the benefit of subscribers and relying parties (end entities)
    - the Memorandum of Understanding (MOU) and Service Level Agreement (SLA) between VANguard and the subscriber
    - the contract for services between VANguard and Symantec.

12. The provisions of the relevant CP and PDS prevail over the provisions of this CPS to the extent of any direct inconsistency.

13. The headings of this CPS follow the framework provided by the *Internet Engineering Task Force Request for Comment 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* (http://ietfreport.isoc.org/idref/rfc3647/).

1.2 Document Name and Identification

14. This document is known as the VANguard CPS. The OIDs for this document are:
    - Production environment: 1.2.36.1.1001.30.1.1
    - Third Party Test environment: 1.2.36.1.1001.40.1.1

    and are based on the following structure:

1	ISO
2	Member Body
36	Australia
1	Government
1001	VANguard
30/40	Business system (VANguard Production and Third Party Test environments)
4/11	Identifies individual object, document etc.
1	Object or document version number, incrementing from 1

15. All OIDs are recorded in the relevant CP and PDS.

1.3 PKI Participants

16. The VANguard PKI participants include Australian, State, Territory, and Local government agencies, as well as suppliers and contractors.

17. These PKI participants are referenced in this document as subscribers and relying parties.

1.3.1 Certificate Authorities (CAs)

18. As part of the VANguard Program, Symantec provides an MPKI service that includes a two tier private Certificate Authority (CA) hierarchy comprising a VANguard Root CA and two (VANguard OCA and Notary CA) subordinate CAs.

19. The function of each subordinate CA is to digitally sign and issue end entity certificate requests that are approved by the Department nominated RA Administrator(s). There are four different types of end entity certificates available in the VANguard Program. Each type of certificate has a unique purpose and is issued under one of the two subordinate CAs.

20. The certificate types issued by the VANguard PKI are as follows:

Certificate Type	Certificate Issuer
VANguard RCA	Self issued
VANguard OCA	VANguard RCA
VANguard Notary CA	VANguard RCA
VANguard Agency Certificate	VANguard OCA
VANguard Authentication Certificate	VANguard OCA
VANguard Notarisation Certificate	VANguard Notary CA
VANguard Assertion Certificate	VANguard Notary CA

21. The four different types of end entity certificates available are described below:

- VANguard Agency Certificate - signed and issued under the VANguard OCA, the VANguard Agency certificates are issued to (and hosted by) authorised Agencies and organisations. These Agency certificates are then used to authenticate to the VANguard Web Services environment and to digitally sign Agency SAML authentication requests.
- VANguard Authentication Certificate - signed and issued under the VANguard OCA, the VANguard Authentication certificates are used to digitally sign SAML responses as well as short lived SAML assertions.
- VANguard Notary Certificate - signed and issued under the VANguard Notary CA, the VANguard Notary private keys reside on HSMs hosted within the Department and are used for the digital time stamping of documents.
- VANguard Assertion Certificate - signed and issued under the VANguard Notary CA, the VANguard Assertion private keys reside on HSMs hosted within the Department and are used to digitally sign long lived SAML assertions.

1.3.2 Registration Authorities (RAs)

22. The VANguard Registration Authority (RA) keys are managed by the Department using RA software provided by Symantec.

23. The RA keys are used to:

- manage the VANguard PKI certificates
- authorise the issue or re-issue of new VANguard certificates
- authorise the revocation of existing VANguard certificates that should no longer be trusted.

1.3.3 Subscribers

24. The subscribers are the PKI participants identified in *Section 1.3 PKI Participants*.

1.3.4 Relying Parties

25. The relying parties are the PKI participants identified in *Section 1.3 PKI Participants*.

1.3.5 Other Participants

26. For some certificate types the relying party may be a Court or an entity testing the veracity of a notarised document.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

27. The appropriate certificate uses are defined in the relevant CP and PDS for each certificate type, and in the MOU and SLA entered into between VANguard and a subscriber.

1.4.2 Prohibited Certificate Uses

28. Prohibited certificate uses are defined in the relevant CP, and in the PDS and SLA entered into between VANguard and the subscriber.

29. In each VANguard certificate the certificate policies extension includes a text field with the following disclaimer:
This certificate is subject to the usage constraints and limitations of liability contained in the PDS & Service Level Agreement. Reliance not expressly permitted in those documents is not supported.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

30. The organisation administering this document is the VANguard Program.

1.5.2 Contact Person

31. Use the 'Contact Us' link on the VANguard website if you have any questions in relation to this CPS: http://www.vanguard.business.gov.au

32. For information regarding CA functions including support contact details and support hours, refer to the applicable Service Level Agreement (SLA).

1.5.3 Person Determining CPS Suitability for the Policy

33. The VANguard Policy Approval Authority (PAA) has determined that this CPS is suitable for use with the relevant CP and PDS. The PAA is responsible for the governance of the PKI within VANguard. Currently the General Manager, VANguard Program, is responsible for all policy approval and management functions and performs this function.

1.5.4 CPS Approval Procedures

34. The PAA is responsible for approving changes to this CPS in accordance with the provisions of *Section 9.12 Amendments*.

1.6 Definitions and Acronyms

35. Refer to the *VANguard Glossary* for a full list of definitions and acronyms.

2 Publication and Repository Responsibilities

2.1 Repositories

36. Symantec is responsible for the management and operation of repository functions related to CA services. This includes the Certificate Directory and Certificate Revocation List (CRL).

2.2 Publication of Certification Information

37. Symantec is responsible for making the VANguard RCA certificate, which contains only the VANguard RCA public key, available to end entities on the VANguard Enrolment Page available on the Symantec website: https://pki.verisign.com.au/services/DepartmentofInnovationIndustryScienceandResearchAustralianAuthenticationandNotaryServicesAgency/digitalidCenter.htm

38. VANguard is responsible for the management of the VANguard website which publishes is read-only access to certificate information.

39. This CPS, the Agency CP, and the Agency PDS policy documents are publicly available online from this website: http://www.vanguard.business.gov.au

2.3 Time or Frequency of Publication

40. Symantec will update the Certificate Directory as soon as practicable whenever a new certificate is issued.

41. Symantec will update the CRL at least once daily.

2.4 Access Controls on Repositories

42. Not applicable.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

43. The VANguard CA will assign an X.500 distinguished name to each issued certificate based on the registration information.

44. The distinguished name to be included in the Subject field of a certificate should be constructed in accordance with requirements for each certificate type, including the common elements shown in the table below. Note that the exception to this is for Agency certificates where the Subject Name fields are nominated by the Agency, and the Organisation (o=) is the Agency name.

Standard Attribute Type	Value
Common Name	cn=<Certificate Type>
Organisational Unit	ou=Australian Authentication and Notary Services
Organisation	o=Australian Government
Country	c=AU

3.1.2 Need for Names to be Meaningful

45. Names must be unambiguous and unique and sufficiently detailed to enable identification of the relevant subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

46. Anonymity and pseudonymity are not supported.

3.1.4 Rules for Interpreting Various Name Forms

47. Distinguished Names must include each of the elements specified in the relevant certificate profile.

3.1.5 Uniqueness of Names

48. Software controls in the Symantec MPKI will ensure that registration names are unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

49. Trademark rights, or other intellectual property (IP) rights, may exist in the Organisation's name, or other parts of the registration information or certificate information.

50. By applying for registration, the subscriber, and the certificate applicant:

    - authorise the VANguard CA to use the relevant IP for the purpose of creating a Distinguished Name, and for other purposes reasonably necessary in relation to the issuance of keys and certificates to, and their use by, the organisation and its subscribers
    - warrant that they are entitled to use that IP for the purposes for which keys and certificates are issued and may be used, without infringing the rights of any other person
    - agree to indemnify the VANguard CA and their respective officers, employees, contractors and agents against loss, damage, costs or expenses of any kind (including legal costs on a solicitor-client basis) incurred by them in relation to any claim, suit or demand in respect of an infringement or alleged infringement of the IP rights of any person.

51. The VANguard CA does not independently check the status of any trademark or other IP rights.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

52. The VANguard CA verifies the certificate applicant's possession of a private key by the following:
    - the use of a digitally signed certificate request (PKCS#10)
    - another cryptographically-equivalent demonstration, or
    - another VANguard-approved method.

53. Where a key pair is generated by the VANguard PKI on behalf of a subscriber (eg where pre-generated keys are placed on an approved hardware security token), this requirement is not applicable.

3.2.2 Authentication of Organisation Identity

54. Refer to the *VANguard Customer Engagement and Integration Procedure*.

3.2.3 Authentication of Individual Identity

55. Refer to the *VANguard Customer Engagement and Integration Procedure*.

3.2.4 Non-verified Subscriber Information

56. See the relevant CP or PDS.

3.2.5 Validation of Authority

57. See the relevant CP or PDS.

3.2.6 Criteria for Interoperation

58. Not applicable.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

59. Certificates are not renewed; however, a new certificate can be applied for with the same Distinguished Name.

3.3.2 Identification and Authentication for Re-key After Revocation

60. Rekey is not permitted after certificate revocation. A certificate holder requiring replacement keys and certificates after revocation must:
    - apply for new keys and certificates
    - comply with all initial registration requirements and procedures.

61. Subscribers applying for the issue of a new certificate after revocation must apply for a new certificate online. VANguard then approves the issuing of this new certificate.

3.4 Identification and Authentication for Revocation Request

62. Before processing a request for revocation of a certificate, the VANguard PKI verifies that the request is made by a person or entity authorised to request revocation of that certificate.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

63. The VANguard RA provides an online enrolment process for the issuance of certificates.

4.1.1 Who can Submit a Certificate Application?

- An organisation can apply to the VANguard RA for a certificate. Note: an organisation can only have one certificate with the same Distinguished Name, although some overlap is provided prior to the expiry of a certificate.
- Before being issued with a certificate, applicants must provide sufficient information for the certificate they are applying for, and be verified in accordance with *Section 3.2 Initial Identity Validation*.

4.1.2 Enrolment Process and Responsibilities

64. The VANguard RA is responsible for:
    - ensuring that an applicant meets the evidence of authentication criteria
    - ensuring authenticity of any document received as evidence of any matter as part of the registration process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

65. The issuing CA and RA perform identification and authentication procedures to validate the certificate application.

4.2.2 Approval or Rejection of Certificate Applications

66. On receiving a request for a certificate, the RA approves or refuses the issuance of a certificate. The RA is not bound to approve the issuance of a certificate despite receipt of an application.

4.2.3 Time to Process Certificate Applications

67. VANguard provides a sub-second response time from when a transaction is received to when it is dispatched from VANguard's internal processor.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

68. The CA, when issuing a certificate, will ensure at the time it issues a certificate that:

- the RA has confirmed that verification has been successfully completed in accordance with *Section 4.1.2 Enrolment Process and Responsibilities*
- the certificate contains all the elements required by the CP or PDS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

69. VANguard will notify subscribers that they have created a certificate, and provide subscribers with access to their certificates.

70. Subscribers will be able to download their certificates from the Symantec VANguard website. Notifications will be by email with direct provision of a certificate at the time of enrolment.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

71. An organisation is deemed to have accepted a certificate when the applicant enters a PIN at a URL that is emailed to the applicant after the CA has signed the certificate. The email address used is that provided in the registration information.

- The applicant must notify the RA of any inaccuracy or defect in the information in a certificate promptly after receipt of the certificate or publication of the certificate in the repository, or upon earlier notice of the information to be included in the certificate.
- The applicant must not create digital signatures using a private key corresponding to the public key listed in a certificate (or otherwise use such private key) if the foreseeable effect would be to induce or allow reliance upon a certificate that has not been accepted.
- Once a certificate is issued, the CA shall have no continuing duty to monitor or investigate the accuracy of the information in a certificate, unless the CA is notified in accordance with the relevant CP or PDS of that certificate’s compromise.
- Certificates will be published after issue as required.

4.4.2 Publication of the Certificate by the CA

72. The CA will update the Certificate Directory as soon as practicable whenever a new certificate is issued.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

73. The CA does not automatically notify other entities of the issuance of the certificate. The CA however does provide a service for entities to look up certificates.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

74. See the relevant CP or PDS.

4.5.2 Relying Party Public Key and Certificate Usage

75. See the relevant CP or PDS.

4.6 Certificate Renewal

76. Certificates will not be renewed; instead they will be reissued before certificate expiry.

4.6.1 Circumstance for Certificate Renewal

77. Not applicable.

4.6.2 Who May Request Renewal

78. Not applicable.

4.6.3 Processing Certificate Renewal Requests

79. Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

80. See *Section 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate*.

81. Not applicable.

4.6.5 Publication of the Renewal Certificate by the CA

82. Not applicable.

4.6.6 Notification of Certificate Issuance by the CA to Other Entities

83. See *Section 4.4.3 Notification of Certificate Issuance by the CA to Other Entities*.

4.7 Certificate Re-key

84. Certificates will not be re-keyed; instead they will be reissued before certificate expiry.

4.7.1 Circumstance for Certificate Re-key

85. Not applicable.

4.7.2 Who May Request Certification of a New Public Key

86. The subscriber, or an authorised representative of a subscriber, can request the certification of a new public key.

4.7.3 Processing Certificate Re-keying Requests

87. Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

88. See *Section 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate*.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

89. See *Section 4.4.1 Conduct Constituting Certificate Acceptance*.

4.7.6 Publication of the Re-keyed Certificate by the CA

90. See *Section 4.4.2 Publication of the Certificate by the CA.*

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

91. See *Section 4.4.3 Notification of Certificate Issuance by the CA to Other Entities*.

4.8 Certificate Modification

92. The VANguard PKI does not support certificate modification. If any information contained within a certificate changes for any reason, the certificate must be revoked. A new certificate may or may not be issued, depending on the circumstances.

4.8.1 Circumstance for Certificate Modification

93. Not applicable.

4.8.2 Who May Request Certificate Modification

94. Not applicable.

4.8.3 Processing Certificate Modification Requests

95. Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

96. See *Section 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate*.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

97. Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

98. Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

99. See *Section 4.4.3 Notification of Certificate Issuance by the CA to Other Entities*.

4.9 Certificate Revocation and Suspension

100. On revocation of a certificate:
    - the certificate's operational period expires
    - the underlying contractual obligations between the organisation and other VANguard PKI entities are unaffected
    - the subscriber must continue to safeguard their private keys unless they destroy their private keys
    - the subscriber must cease using the certificate for any purpose whatsoever
    - the CA must promptly notify the subscriber that its certificate has been revoked
    - the CA must update the CRL.

4.9.1 Circumstances for Revocation

101. The RA will revoke a certificate (whether or not it has received a request to do so) where it becomes aware (or reasonably suspects) that:
    - there has been a loss, theft, modification, or other compromise of the associated private key
    - faulty or improper registration, key generation or issue of a certificate has occurred
    - a change in the registration information occurs
    - the certificate's associated private key or other trustworthy system was compromised in a manner materially affecting the certificate's reliability
    - the applicable subscriber has not complied with an obligation under the CPS, the relevant CP, PDS, or the SLA, or
    - another person's information has been or may be materially threatened or compromised unless the certificate is revoked.

102. The RA will also revoke a certificate:
    - on request by a person specified in *Section 3.2.5 Validation of Authority*, or
    - if it becomes aware that the subscriber has ceased to belong to the Community of Interest.

4.9.2 Who Can Request Revocation

103. A subscriber, or an authorised representative of a subscriber, or an authorised representative of the organisation including any Authorised Officer of the organisation, can request the RA to revoke the certificate(s) at any time.

104. The RA may require such proof as it deems reasonably necessary to confirm the identity of the individual requesting revocation of a certificate, and if it is not the Authorised Officer, its relationship with the subscriber.

105. A request (including an order or direction) from any entity other than those set out in this section, for revocation of a certificate will be processed only if the RA is satisfied that the entity:
    - is lawfully empowered to require revocation of the certificate, or
    - is lawfully entitled to administer the organisation's affairs which relate to the certificate(s).

106. Subscribers and relying parties can request revocation of their certificates. However, subscribers and relying parties must not be in a position to revoke their own certificates without VANguard's knowledge. This is because VANguard uses the certificates as trust points internally and does not check the CRL.

107. A request for revocation can be verified in the following ways:
    - the request is digitally signed with the private key of an Authorised Officer
    - the request is made in person, and the authority of the requestor is verified
    - the request is made using a Challenge Phrase provided by the applicant at the time of registration.

4.9.3 Procedure for Revocation Request

108. A revocation request, other than one that is made in person, must be sent to the RA by any of the methods described in *Section 9.11 Individual Notices and Communications with Participants*.

109. The CAs will:
    - employ personnel who possess the expert knowledge, experience, and qualifications necessary for the provision of the certification services, and in particular, personnel who possess competence at managerial level, expertise in Digital Signature technology, and familiarity with proper security procedures
    - apply administrative and management procedures which are appropriate for the activities being carried out
    - use trustworthy systems and evaluated products which are protected against modification, and ensure the technical and cryptographic security of the process supported by them
    - ensure that all relevant information concerning a certificate is recorded (electronically or otherwise) for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

4.9.4 Revocation Request Grace Period

110. Requests for revocation should be lodged as soon as the need for revocation becomes apparent, and should not exceed one working day.

4.9.5 Time Within Which CA Must Process the Revocation Request

111. Revocation requests are processed immediately upon receipt from the RA.

4.9.6 Revocation Checking Requirement for Relying Parties

112. See *Section 9.6.4 Relying Party Representations and Warranties.*

4.9.7 CRL Issuance Frequency (if applicable)

113. CRLs are issued every 12 hours (noon and midnight), and are valid for 24 hours.

114. CRLs can also be issued on an emergency basis, as determined by the CA.

4.9.8 Maximum Latency for CRLs (if applicable)

115. One day.

4.9.9 Online Revocation/ Status Checking Availability

116. No stipulation.

4.9.10 Online Revocation Checking Requirements

117. No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

118. No stipulation.

4.9.12 Special Requirements Re Key Compromise

119. The CA will use commercially reasonable efforts to notify potential subscribers and relying parties if the CA discovers, or has reason to believe, that there has been compromise of the private key of a CA or RCA.

4.9.13 Circumstances for Suspension

120. Certificate suspension is not supported by the VANguard PKI.

4.9.14 Who Can Request Suspension

121. Not applicable.

4.9.15 Procedure for Suspension Request

122. Not applicable.

4.9.16 Limits on Suspension Period

123. Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

124. A subscriber or relying party will be able to ascertain the status of a certificate by consulting the Certificate Directory and the CRL.

125. This information is in the Repository. See *Section 2.1 Repositories*.

4.10.2 Service Availability

126. Refer to the applicable SLA.

4.10.3 Optional Features

127. No stipulation.

4.11 End of Subscription

128. No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

129. Subscribers are responsible for their own arrangements regarding key escrow.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

130. No stipulation.

5 Facility, Management, and Operational Controls

131. This section details the controls in place at the Symantec Gatekeeper accredited secure facility in Melbourne. This facility is where the operations and management of the VANguard CAs are undertaken.

132. Where VANguard staff have a direct role in maintaining the security of the VANguard PKI this is mentioned in the relevant sub-section.

5.1 Physical Security Controls

133. Symantec's Gatekeeper accredited *Protective Security Plan* (PSP) details the physical controls in place for the VANguard CA systems, and includes information on:

- site location and construction
- physical access
- power and air conditioning
- water exposures
- fire prevention and protection
- media storage
- waste disposal
- off-site backup
- safe hand carriage
- intruder detection systems.

134. The PSP is a classified document and contains sensitive information not detailed in this document; however, a general overview is provided to describe controls in place.

5.1.1 Site Location and Construction

135. Sites at which certificate services occur, including issuing, revoking and managing certificates, meet or exceed the Australian Government requirements for the processing and storage of classified information.

5.1.2 Physical Access

136. Symantec CA systems are protected by a minimum of four tiers of physical security, with the lower tier required before gaining access to the higher tier.

137. Mandatory access controls are in place that provide successively more restricted access and greater physical security depending on the sensitivity of the material held in a particular area.

138. In addition to the tiered security model, access to keying material is restricted in accordance with Symantec's segregation of duties requirements. Audit logs of access are kept.

5.1.3 Power and Air Conditioning

139. Each site has backup power supplies including diesel generators as a fail-safe power supply. The generators provide power on a priority basis to key services and areas.

5.1.4 Water Exposures

140. Sites are constructed to prevent floods and water damage.

5.1.5 Fire Prevention and Protection

141. Sites are constructed and equipped to extinguish fires and prevent fire damage.

5.1.6 Media Storage

142. Media containing information on the VANguard CAs is stored in a manner to prevent that information being used or accessed by unauthorised personnel. Material is stored in appropriate security containers related to its classification level.

5.1.7 Waste Disposal

143. Records containing personal information are destroyed. Shredders are available at the sites.

5.1.8 Off-site Backup

144. A backup of key records is kept externally in a bank safe.

5.2 Procedural Controls

5.2.1 Trusted Roles

145. Symantec staff involved in VANguard CA operations are identified as Positions of Trust in the Symantec *Trusted Employee Policy*. This policy describes the procedures that are implemented to ensure that appropriate screening is performed.

146. The screening varies with the duties staff must perform.

5.2.2 Number of Persons Required Per Task

147. All cryptographic activity takes place in the presence of two or more trusted staff members who have been authorised for the purpose.

5.2.3 Identification and Authentication for Each Role

148. The Symantec PSP specifies identification and authentication requirements, which must be met before a person can perform the roles and functions of a Position of Trust.

5.2.4 Roles Requiring Separation of Duties

149. Roles requiring Separation of Duties include (but are not limited to):
    - the validation of information in certificate applications
    - the acceptance, rejection, or other processing of certificate applications, revocation requests, or enrolment information
    - the issuance, or revocation of certificates, including personnel having access to restricted portions or the repository
    - the handling of subscriber information or requests
    - the generation, issuing or destruction of a CA certificate
    - the loading of a CA on production.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

150. All Symantec staff occupy a Position of Trust and are vetted through a process described in the Symantec *Trusted Employee Policy*.

151. Symantec has established and maintains a position of Facility Security Officer for its Gatekeeper accredited facility.

152. Staff having access to personal information are cleared to Negative Vetting Level 1 (NV1) in accordance with Gatekeeper requirements. Positions that require NV1 status are specified in the Symantec *Trusted Employee Policy.*

153. VANguard staff are cleared to Baseline as per the Department's Employment Procedures. Staff with access to cryptographic material are cleared to NV1.

5.3.2 Background Check Procedures

154. Background checks for security clearances to the level of NV1 are carried out in accordance with the Gatekeeper procedures and Australian Government security requirements.

5.3.3 Training Requirements

155. Requirements for training of Symantec staff are set out in the relevant *Symantec Operations Manual*.

5.3.4 Retraining Frequency and Requirements

156. Symantec staff are provided with refresher training to ensure that they maintain the level of proficiency required to perform their job.

5.3.5 Job Rotation Frequency and Sequence

157. Jobs are not rotated due to the varying security requirements of each role, and the substantial technical knowledge required to perform tasks. Additional controls are in place to detect and prevent fraudulent activities.

5.3.6 Sanctions for Unauthorised Actions

158. The *Symantec Trusted Employee Policy* and the *Symantec Employee Handbook* detail appropriate sanctions for unauthorised actions by Symantec staff.

159. VANguard staff are subject to disciplinary sanctions under the terms of their employment for any unauthorised actions.

5.3.7 Independent Contractor Requirements

160. *Section 5.3 Personnel Controls* applies to any staff member within VANguard CAs' operations.

5.3.8 Documentation Supplied to Personnel

161. All staff involved in the operations of the VANguard CAs and RA have access to the approved documents that are relevant to their duties.

5.4 Audit Logging Procedures

162. The Symantec PSP details the audit logging procedures required to maintain a secure environment.

5.4.1 Types of Events Recorded

163. The following events are recorded in audit log files:
    - system start-up and shutdown
    - CA/RA application start-up and shutdown
    - attempts to create, remove, or set passwords, or change the system privileges of users performing Trusted Roles
    - changes to CA and RA details and/or keys
    - login and logoff attempts
    - unauthorised attempts to gain access to the network of the CA and RA system
    - generation of own and subordinate CA and RA keys
    - issuance and revocation of certificates.

164. The following events are logged, either electronically or manually:
    - key generation ceremonies and key management databases
    - physical access logs
    - system configuration changes and maintenance
    - discrepancy and compromise reports
    - records of the destruction of media containing key material or personal information of subscribers.

5.4.2 Frequency of Processing Log

165. Symantec will review its audit logs in response to alerts based on irregularities and incidents within the VANguard CA and RA system. Symantec will also compare the audit logs against other manual and electronic logs in response to suspicious actions.

5.4.3 Retention Period for Audit Log

166. Audit logs will be retained for at least 15 days after processing and then archived.

5.4.4 Protection of Audit Log

167. Electronic audit logs are protected against unauthorised viewing, modification, deletion and other tampering by storage in a trustworthy system.

5.4.5 Audit Log Backup Procedures

168. Electronic audit logs are backed up every 15 minutes and fully backed up overnight.

5.4.6 Audit Collection System (Internal vs External)

169. The audit collection system is maintained internally.

5.4.7 Notification to Event-Causing Subject

170. There will not necessarily be notification of the occurrence of an audit event. Notification will only be performed where VANguard believes the circumstances require it.

5.4.8 Vulnerability Assessments

171. The VANguard Security Manager (SM) may conduct vulnerability assessments of the VANguard PKI if required by the VANguard General Manager (GM).

172. Symantec will be informed of any internal vulnerability assessment prior to its commencement to minimise disruption of the VANguard services.

5.5 Records Archival

173. The Symantec PSP includes general records archival and records retention policies.

174. VANguard will maintain records, including documentation of actions and information that is relevant to each certificate application, including:
    - the identity of the applicant named in each certificate
    - the identity of persons requesting certificate revocation
    - other facts represented in the certificate
    - time stamps
    - any other material facts related to issuing certificates.

175. Records may be kept in either computer-based information or paper-based documents, with accurate, secure and complete indexing, storage, and preservation.

5.5.1 Types of Records Archived

176. Most of the information collected by the VANguard RA is archived. See *Section 5.4.1 Types of Events Recorded.*

5.5.2 Retention Period for Archive

177. Records are retained in relation to certificates (including personal information) for seven years after the date the certificate expires or is revoked. See the VANguard Privacy Policy on http://www.vanguard.business.gov.au

5.5.3 Protection of Archive

178. Only trusted staff are able to access the archive. Archived records are protected against unauthorised viewing, modification, deletion and other tampering by storage in a trustworthy system.

5.5.4 Archive Backup Procedures

179. Electronic archives are backed up every 15 minutes and fully backed up overnight.

5.5.5 Requirements for Time Stamping of Records

180. All automatically generated logs are time stamped using the system clock of the computer on which they were generated.

181. The following records are time stamped:
    - certificates
    - CRLs and other revocation databases
    - customer service messages.

5.5.6 Archive Collection System (Internal or External)

182. The archive collection system is maintained internally.

183. Archiving is performed by the operations personnel delegated with that responsibility.

5.5.7 Procedures to Obtain and Verify Archive Information

184. VANguard can provide access to archived information, including confidentiality and personal information, on request and subject to the other provisions in this CPS.

5.6 Key Changeover

185. Key changeover occurs when the subscriber needs to obtain new keys after expiry of a VANguard cryptographic key.

186. Key changeover for subordinate CAs involves the VANguard RCA confirming the identity of the subordinate CA and performing a key generation ceremony after which the subordinate CA's key pair is replaced with the new key pair.

187. The RCA, OCA, and RA will ensure that key changeover causes minimal disruption to subscribers, and provide subscribers with reasonable notice of any planned changeover.

188. During this changeover both authentication public keys in the associated certificate will be in use and published in the Certificate Directory.

5.7 Compromise and Disaster Recovery

189. Symantec maintains a *Disaster Recovery and Business Continuity Plan* (DR&BCP) covering all reasonably foreseeable types of disasters and compromises affecting the certificate services under this CPS including:
    - loss or corruption (including suspected corruption) of computing resources, software, and/or data of the VANguard CAs
    - compromise of the VANguard CA private keys which relying parties rely on to establish trust in certificates.

190. The Symantec DR&BCP is consistent with the requirements of the Symantec PSP. For security reasons these documents are not publicly available.

5.7.1 Incident and Compromise Handling Procedures

191. Where a suspected or known security incident has occurred Symantec will immediately inform VANguard and implement the procedures in the Symantec DR&BCP.

192. VANguard at its discretion may report security incidents to subscribers and relying parties if the assurance of the VANguard PKI is compromised.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

193. The processes outlined in the Symantec DR&BCP will be performed if computing resources, software and/or data are corrupted.

5.7.3 Entity Private Key Compromise Procedures

194. If a subordinate CA's private key is compromised, the VANguard RCA will revoke the CA's certificate, and report it. See *Section 5.7.1 Incident and Compromise Handling Procedures.*

195. If a key pair of a VANguard CA is revoked (including as a result of compromise), the revocation will be reported in the CRL and in the repository.

5.7.4 Business Continuity Capabilities After a Disaster

196. The Symantec DR&BCP sets out response and recovery procedures for each type of disaster or compromise.

5.8 CA or RA Termination

197. This sub-section applies if VANguard becomes aware that it, or Symantec, intends to or is likely to, cease providing services which are:
    - necessary for the issue of keys and certificates under this CPS, or
    - necessary for reliance on Digital Signatures or certificates.

198. VANguard will give as much notice as possible of the relevant circumstances, and the actions it proposes to take to:
    - all subscribers
    - the relying parties of which VANguard is aware.

199. Where Symantec intends to, or is likely to cease providing services, provisions in the Contract between Symantec and VANguard will be implemented.

200. In the circumstances described in *Section 4.10.1 Operational Characteristics*, each PKI Service Provider must co-operate with each other in minimising disruption to the services provided under this CPS and to the affected parties.

201. Where VANguard intends to terminate its own services, it will attempt to give at least three months notice to the affected parties.

202. If Symantec unexpectedly ceases providing services referred to above, VANguard must immediately give notice to the affected parties.

203. If any personal information is transferred from one PKI Service Provider to another, each relevant PKI Service Provider must ensure that the information is protected as required under *Section 9.4 Privacy of Personal Information*.

204. The obligations under this section are in addition to any obligations the Department's VANguard CA or any other entity has under the requirements of *Section 9.6 Representations and Warranties.*

205. The termination of a VANguard CA is subject to the contract entered into between Symantec and VANguard.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

206. Key pair generation is performed using systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorised use of those keys.

207. Key pair generation is performed in accordance with the *Key Management Plan* (KMP), and the *VANguard Customer Engagement and Integration Procedure.*

208. Keys for the CAs are generated by the RCA; keys for subscribers are generated by the RA.

6.1.2 Private Key Delivery to Subscriber

209. The VANguard PKI does not deliver its CA private keys to any entity.

210. Refer to the relevant CP and PDS for subscriber private key delivery information.

6.1.3 Public Key Delivery to Certificate Issuer

211. See *Section 4.3 Certificate Issuance*.

6.1.4 CA Public Key Delivery to Relying Parties

212. CA public keys delivery to relying parties meets the *IETF RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)* standard, and is available to download from the repository.

213. See the relevant CP.

6.1.5 Key Sizes

214. The VANguard PKI key strengths are a minimum 1024 bits in length. The VANguard RCA keys strengths are a minimum 2048 bits in length.

215. A trustworthy hardware device operating within a processing centre is used to create, protect, and store each subordinate CA private keys, and the RCA private key.

6.1.6 Public Key Parameters Generation and Quality Checking

216. Public key parameters generation and quality checking is ensured through the use of a product listed on the Evaluated Products List (EPL).

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

217. Key usage is defined in accordance with X.509 v3.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

218. The VANguard PKI uses mechanisms detailed in the KMP to protect its private keys from loss, disclosure, modification or unauthorised use.

6.2.1 Cryptographic Module Standards and Controls

219. VANguard maintains and uses industry standard specialised cryptographic hardware security modules (HSMs).

220. Cryptographic modules used in the VANguard PKI are designed to ensure the integrity and security of hardware key management.

6.2.2 Private Key (n out of m) Multi-person Control

221. VANguard does not use multi-person controls.

6.2.3 Private Key Escrow

222. The VANguard PKI does not escrow its CA private keys.

6.2.4 Private Key Backup

223. The VANguard PKI backs up the private keys of the CAs. These backups are stored in the VANguard CA secure facility, as well as an external secure location to ensure data recovery.

224. Private key backup is not provided for subscribers.

6.2.5 Private Key Archival

225. The VANguard PKI keeps a copy of all private keys it has used.

226. A private key archive is not provided for subscribers, relying parties, or end user subscribers.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

227. The detail of how the VANguard PKI manages its private keys and how these are stored in cryptographic modules is sensitive information and is not detailed in this document.

6.2.7 Private Key Storage on Cryptographic Module

228. A trustworthy hardware device operating within a processing centre is used to create, protect, and store the VANguard PKI private keys.

6.2.8 Method of Activating Private Key

229. Activation of the RCA private key requires multi-person control.

6.2.9 Method of Deactivating Private Key

230. When a CA is taken offline, the token containing the CA private key is removed from the reader in order to deactivate it.

6.2.10 Method of Destroying Private Key

231. Private keys are destroyed in a way that prevents their loss, theft, modification, unauthorised disclosure, or unauthorised use.

6.2.11 Cryptographic Module Rating

232. Cryptographic modules used in the VANguard PKI use software listed on the Australian Signals Directorate (ASD) EPL.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

233. The VANguard CA archives the public keys of its CAs. The archived public keys are located in the repository and are stored for seven years in accordance with the *Australian National Archives Policy*.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

234. The usage period for the CA public and private keys is 14 years.

235. The usage period for the subscriber public and private keys is four years.

6.4 Activation Data

236. No activation data other than access control mechanisms are required to operate cryptographic modules.

6.4.1 Activation Data Generation and Installation

237. Not applicable.

6.4.2 Activation Data Protection

238. Not applicable.

6.4.3 Other Aspects of Activation Data

239. Not applicable.

6.5 Computer Security Controls

240. The *VANguard Risk Management Plan* (RMP) covers security of the Symantec CA operations and systems used to provide computer security.

241. All PKI service providers should use only trustworthy systems in performing their respective services.

6.5.1 Specific Computer Security Technical Requirements

242. Systems that operate the CA software and store data files use trustworthy systems to secure against unauthorised access.

243. Production servers used to support VANguard certificates operate on their own hardware and software platforms and are not generally accessible or available for other uses.

6.5.2 Computer Security Rating

244. Trustworthy systems used to perform CA or RA functions must meet the requirements of the Australian Government's information security standards.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

245. Symantec has in place a software development lifecycle that addresses all aspects of secure software development for its CA and RA software.

6.6.2 Security Management Controls

246. Symantec has in place security management tools and controls to ensure the confidentiality, integrity, and availability of its CA and RA software and hardware.

6.6.3 Life Cycle Security Controls

247. The detail of the VANguard CA lifecycle security controls is sensitive information and is not detailed in this document.

6.7 Network Security Controls

248. The VANguard CA uses firewalls for securing network access, encryption to secure the communication of sensitive information and confidentiality, and digital signatures for non-repudiation and authentication.

249. Network security controls are specified in the Symantec PSP and the RMP which identify and address all high or significant life cycle security threats.

6.8 Time-Stamping

250. Symantec uses a trusted time source for ensuring a consistent network time across Symantec systems.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

251. The relevant CP contains the certificate profile for the VANguard PKI, and the relevant PDS contains the certificate profile for end entity certificates.

7.1.1 Version Number(s)

252. The VANguard PKI supports and uses Version 3 certificates.

7.1.2 Certificate Extensions

253. The VANguard PKI supports and uses Version 3 certificate extensions.

7.1.3 Algorithm Object Identifiers

254. The VANguard PKI uses only those cryptographic algorithms approved by ASD.

255. OIDs are not allocated to algorithms in the VANguard PKI.

7.1.4 Name Forms

256. See the relevant CP for the full Distinguished Name of the CA issuing the certificate in the 'Issuer Name' field of the certificate profile.

7.1.5 Name Constraints

257. Anonymous or pseudonymous names are not supported.

7.1.6 Certificate Policy Object Identifier

258. The OID for each CP or PDS under which a certificate is issued is contained in the standard extension field of issued X.509 v3 certificates.

259. See the relevant CP or PDS.

7.1.7 Usage of Policy Constraints Extension

260. Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

261. The VANguard PKI supports the use of policy qualifiers syntax and semantics.

262. See the relevant CP or PDS.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

263. The VANguard PKI supports the use of syntax and semantics policy qualifiers as indicated in the relevant CP or PDS.

264. This policy does not require the CP extension to be critical.

265. The X.509 CP complies with the Australian standard X.509 profile.

7.2 CRL Profile

266. The location of the CRL for a certificate is published in the certificate extension field of the certificate named 'CRL Distribution Point'.

7.2.1 Version Number(s)

267. The VANguard PKI supports and uses X.509 Version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

268. The VANguard PKI supports and uses X.509 Version 2 CRL entry extensions as indicated in the CRL profile.

7.3 OCSP Profile

269. OCSP functionality is not enabled for certificates created under the VANguard PKI.

7.3.1 Version Number(s)

270. Not applicable.

7.3.2 OCSP Extensions

271. Not applicable.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

272. Symantec's Gatekeeper CA operations and management are audited annually by a Gatekeeper authorised auditor. VANguard processes are covered by this audit.

273. The VANguard SM may conduct audits of a CA or RA if required by the VANguard GM.

274. The VANguard SM is responsible for ensuring the security of VANguard operations and is appointed by the VANguard GM.

8.2 Identity/Qualifications of Assessor

275. VANguard will conduct an Infosec - Registered Assessor Program (IRAP) assessment against the requirements of the *Australian Government Information Security Manual* (ISM).

276. VANguard has a listing with Gatekeeper to operate as a Validation Authority.

8.3 Assessor's Relationship to Assessed Entity

277. IRAP and Gatekeeper auditors will be independent of the audited entity.

278. The VANguard SM is not directly involved in the management of the VANguard PKI and therefore is independent of the audited entity.

8.4 Topics Covered by Assessment

279. The purpose of an IRAP assessment is to be provided with a statement of compliance with DSD and Australian Government policy and best practice standards.

280. The purpose of a Gatekeeper audit is to ensure that a VANguard CA and the VANguard RA:

- maintains compliance with security requirements as per the contract between Symantec and VANguard
- continues to operate as required by the approved documents.

8.5 Actions Taken as a Result of Deficiency

281. Deficiencies found by the VANguard SM will be reported to the VANguard GM who will communicate to the VANguard team and/or Symantec to address identified issues.

8.6 Communication of Results

282. VANguard may release information to subscribers if the information will affect the assurance of the VANguard PKI.

283. The date on which the Symantec Gatekeeper CA was last audited will be published on the Symantec Gatekeeper website, and may also be published by the Department of Finance and Deregulation.

284. The results of a Gatekeeper audit are confidential and will be communicated by the auditor only to the Department of Finance and Deregulation and the audited entity.

285. Results of the compliance audit of the Symantec CA may be released at the discretion of Symantec management.

9 Other Business and Legal Matters

286. Refer to the relevant CP and PDS.

9.1 Fees

287. No fees will be charged unless otherwise stated in the CP or PDS under which the certificates are issued.

9.1.1 Certificate Issuance or Renewal Fees

288. Not applicable.

9.1.2 Certificate Access Fees

289. Not applicable.

9.1.3 Revocation or Status Information Access Fees

290. Not applicable.

9.1.4 Fees for Other Services

291. There may be costs associated where Agencies wish to use certificates for their own programs. See the relevant SLA.

9.1.5 Refund Policy

292. Not applicable.

9.2 Financial Responsibility

293. Refer to the relevant CP and PDS.

9.2.1 Insurance Coverage

294. No stipulation.

9.2.2 Other Assets

295. No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

296. VANguard does not offer a program of insurance to its subscribers.

9.3 Confidentiality of Business Information

297. Refer to the relevant CP and PDS.

9.3.1 Scope of Confidential Information

298. Information released to subscribers or relying parties by VANguard may be considered confidential.

299. Refer to the MOU and SLA between VANguard and the subscriber.

9.3.2 Information not Within the Scope of Confidential Information

300. Information regarding security incidents and/or breaches may be released to the appropriate Government authorities without notification to subscribers or relying parties. VANguard may at its discretion release this information to subscribers and relying parties where such a release does not impact upon any investigation or legal proceeding.

9.3.3 Responsibility to Protect Confidential Information

301. Refer to the SLA.

9.4 Privacy of Personal Information

302. VANguard will uphold the information privacy principles contained in the *Privacy Act 1988 (Cth)*, as well as relevant privacy-related sections of the *Public Service Act 1999, Archives Act 1983*, and other relevant Acts.

303. *Section 9.3 Confidentiality of Business Information* does not apply to personal information.

9.4.1 Privacy Plan

304. VANguard conducts periodic privacy assessments on the specifics as to what information is considered private, and what policies are in place to appropriately handle private information.

305. Refer to the VANguard Privacy Policy which contains the overarching principles and policies that VANguard employs to manage information that passes though VANguard.

9.4.2 Information Treated as Private

306. Personal information is treated as private. Personal information means information or an opinion, whether true or not, and whether materially recorded or not, about an individual that is apparent or can be reasonably ascertained.

9.4.3 Information Not Deemed Private

307. Subscribers agree to the publication, through the Certificate Directory and CRL, of any personal information which forms part of the certificate information.

9.4.4 Responsibility to Protect Private Information

308. The registration information may contain personal information about key holders.

309. The relevant RA must not collect any personal information about key holders as part of the registration process other than the registration information and other necessary information to complete the transaction.

310. In relation to any dealings with personal information collected from certificate applicants:
    - where the services are being provided to or in relation to a Commonwealth Agency the relevant RA agrees to comply with the information privacy principles
    - where the services are provided to a State or Territory Agency then the relevant RA agrees to comply with:
        a. the legislative privacy regime applicable to the VANguard OCA as a contractor to that Agency, or
        b. any other privacy regime which that Agency requires the VANguard OCA to comply with whether this requirement appears in a services contract or otherwise, to the extent the Agency's requirements are consistent with any applicable legislative provisions, and
    - where the services are provided to a private sector entity, the relevant RA agrees to comply with:
        c. the national privacy principles as those principles appear in the *Privacy (Private Sector) Amendment Act 2000*, or
        d. any applicable industry privacy code, so long as that code has been approved by the Federal Privacy Commissioner.

9.4.5 Notice and Consent to Use Private Information

311. Users provide their consent via the VANguard Front End Web (FEW) website to which agencies can send their business users to be authenticated.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

312. Information retained by the VANguard system will only be disclosed under instruction from an appropriate law enforcement body, court, or because of a legislative requirement, or as otherwise required or permitted by law.

9.4.7 Other Information Disclosure Circumstances

313. VANguard will use collected information only for the purpose for which it was collected, unless authorised to do so by the information provider. Agencies will have access to any reports pertaining to their own transactions.

9.5 Intellectual Property Rights

314. All intellectual property rights in any CPS, CP or PDS, or other document published by the VANguard PKI, belong to and will remain the property of the Department. The use of these documents in the preparation of this CPS is acknowledged:

    - Chokhani, Ford, Sabett and Wu, *RFC 3647 : Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, The Internet Society, 2003
    - American Bar Association, *PKI Assessment Guidelines,* 2003.

315. Unless otherwise agreed between the relevant PKI entities:
    - intellectual property rights (IP rights) in the approved documents, the Certificate Directory and the CRL are owned by VANguard

- IP rights in certificates are owned by VANguard, subject to any pre-existing IP rights which may exist in the certificates or the certificate information
- any IP rights in key pairs are owned by Symantec.

316. Symantec which owns IP rights in certificates, Distinguished Names, and key pairs, grants to any other relevant PKI entity which has a requirement under this CPS, the relevant CP, PDS, or other approved documents, to use that IP, the rights it reasonably requires to perform that entity's roles, functions and obligations under this CPS, the relevant CP, PDS, or other approved documents.

317. The PKI entity that owns the relevant IP rights warrants that:
    - it has the rights necessary to grant the licences
    - the use by PKI entities of the relevant IP pursuant to the CPS, the relevant CP, PDS, or other approved documents, will not infringe the IP rights of a third party.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

318. The Root CA for the purposes of this CPS is the VANguard RCA.

319. The VANguard RCA will:
    - establish a chain of trust by issuing a certificate called the VANguard RCA which is a self-signed certificate
    - ensure that the VANguard RCA signs any subordinate CAs issued under the VANguard PKI hierarchy
    - properly conduct the verification process described in *Section 3.2 Initial Identity Validation*
    - ensure the accuracy and completeness of any part of the certificate information which is generated or compiled by the VANguard RA
    - ensure that all relevant information concerning a certificate is recorded (electronically or otherwise) for an appropriate period of time (in the case of certificates being issued to an Agency, as specified in policies and guidelines issued by the National Archives of Australia under the *Archives Act 1983 (Cth*)), and in particular, for the purpose of providing evidence for the purposes of legal proceedings
    - utilise trustworthy systems, procedures and human resources in performing its services
    - comply with any other relevant provisions of the relevant CP or PDS, and other approved documents.

320. The RCA will operate according to the requirements of this CPS and any applicable SLA.

321. The VANguard PKI will ensure at the time it issues a certificate, that the certificate contains all the elements required by the CP or PDS.

322. The VANguard PKI will manage their keys in accordance with *Section 6.2 Private Key Protection and Cryptographic Module Engineering Controls.*

323. The VANguard PKI cannot ascertain or enforce any particular private key protection requirements of any organisation or subscriber.

324. The VANguard PKI will:
    - ensure the availability of a Certificate Directory and CRL
    - promptly revoke a certificate if required.

9.6.2 RA Representations and Warranties

325. The RA will operate according to the requirements of this CPS and any applicable SLA.

9.6.3 Subscriber Representations and Warranties

326. See the relevant PDS and the MOU between VANguard and the subscriber.

9.6.4 Relying Party Representations and Warranties

327. Before relying on a certificate or a digital signature, relying parties must:
    - validate the certificate and digital signature (including by checking whether or not it has been revoked, expired or suspended)
    - ascertain and comply with the purposes for which the certificate was issued and any other limitations on reliance or use of the certificate which are specified in the certificate and the relevant PDS.

328. If a relying party relies on a digital signature, or certificate, in circumstances where it has not been validated, it assumes all risks with regard to it (except those that would have arisen had the relying party validated the certificate), and is not entitled to any presumption that the digital signature is effective as the signature of the subscriber or that the certificate is valid.

329. Relying parties must also comply with any other relevant obligations specified in this CPS including those imposed on the entity when it is acting as a subscriber.

330. Additionally, the relying party should consider the certificate type. The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party.

9.6.5 Representations and Warranties of Other Participants

331. See the relevant CP or PDS.

9.7 Disclaimers of Warranties

332. The VANguard business model does not provide for certificates with different levels of assurance or suitability for use up to pre-determined financial limits. VANguard does not accept any liability in relation to the operations of the VANguard PKI.

333. No implied or express warranties are given by the Department, or by any other entity who may be involved in the issuing or managing of VANguard key pairs and certificates, and all statutory warranties are to the fullest extent permitted by law expressly excluded.

334. See the relevant PDS and the MOU between VANguard and the subscriber.

9.8 Limitations of Liability

335. See the relevant CP, PDS, and the MOU between VANguard and the subscriber.

336. Symantec and VANguard limitations of liability are covered in the Contract.

9.9 Indemnities

337. See the relevant PDS and the MOU between VANguard and the subscriber.

338. Symantec and VANguard indemnities are covered in the Contract.

9.10 Term and Termination

9.10.1 Term

339. The provisions of this CPS are in effect once approved by the PAA and published on the VANguard website: http://www.vanguard.business.gov.au

340. The provisions of this CPS and the relevant CP or PDS remain in effect until the expiry or revocation of the last issued certificate if not terminated sooner.

9.10.2 Termination

341. The Department may terminate the VANguard PKI at its own discretion, or otherwise as may be required by the Australian government.

342. The Department will notify subscribers, relying parties, and other participants, of the intended termination of the VANguard PKI.

9.10.3 Effect of Termination and Survival

343. Provisions described as having an ongoing operation survive the termination or expiration of the relevant contractual relationship between any PKI entities.

9.11 Individual Notices and Communications with Participants

344. Notices to subscribers must be sent to the physical, postal, facsimile or email address of the subscriber, which is included in its registration information, or to another address which the subscriber has specified to the sender.

345. A notice to any entity in relation to this CPS, CP or PDS, must be signed by the sending entity. If the notice is sent electronically it must be digitally signed.

346. A notice sent is taken to be received:

- if it is hand-delivered to a physical address at the time of delivery whether or not any person is there to receive it
- if it is posted by prepaid post at 5pm on the third day after it is posted even if the notice is returned to the sender
- if it is transmitted by facsimile when the sending machine produces a report showing the transmission was successful
- if it is sent by email when it enters a system under the control of the addressee.

347. If, under the previous paragraph, a notice would be taken to be received outside normal business hours at the addressee's place of business, the parties agree in these circumstances that it is actually taken to be received at 9am on the next business day at that place.

9.12 Amendments

9.12.1 Procedure for Amendment

348. The following process describes how changes to an approved document may be affected:

- a change request is formulated by the person requesting the change identifying the relevant approved document to be changed, stating the amendments suggested, and describing the impact (if any) on the operation of the VANguard CAs and/or RAs
- the change is submitted to the PAA, which reviews the change request, assesses whether the change request is required, and approves the changes

- VANguard will update the repository to reflect the current version of all publicly accessible approved documents so that end entities can obtain current versions of all publicly accessible approved documents.

349. New documents for which approval is sought must follow the same process above; however, instead of providing details of the changes requested, the document that is sought to be approved must be provided to the PAA.

350. If a change is made to this CPS that materially affects the assurance provided, then it may be necessary for the VANguard CA to modify the CP or PDS OID. If this occurs, the VANguard CA will contact affected subscribers.

9.12.2 Notification Mechanism and Period

351. There will not be any formal notification process. Rather, notification will follow a 'pull' model, requiring authorised parties to monitor the CPS, CP or PDS, or other approved documents at their discretion and inspect new versions upon release.

352. VANguard will maintain all publicly accessible approved documents in the repository. Changes to all publicly accessible approved documents will also be published in the repository.

353. VANguard will inform Symantec of all changes to approved documents directly, and will use reasonable endeavours to do this.

9.12.3 Circumstances Under Which OID Must Be Changed

354. If an approved change to this CPS materially affects the assurance provided then the (Policy) OID may be changed. If this occurs then VANguard will contact affected subscribers. Otherwise where a change to a CPS, CP, or PDS is required, the OID of the policy will stay the same, and the CPS or CP will be provided with a new version number.

355. A new OID must be given when a new CP or PDS is created for a different Community of Interest.

9.13 Dispute Resolution Procedures

356. If a dispute arises between any PKI entity (dispute) either PKI entity to the dispute may, by written notice to the other PKI entity, specify the details of the dispute (Dispute Notice).

357. If a Dispute Notice is given, then the PKI entity must promptly meet and negotiate in good faith to resolve the dispute.

358. If the dispute remains unresolved 30 days after receipt of the Dispute Notice, the PKI entities agree to submit the dispute to mediation administered by, and in accordance with, the mediation rules of the Australian Commercial Disputes Centre (ACDC). A single mediator will be agreed by the PKI entities or, failing agreement, appointed by the ACDC. The mediation will be held in Canberra and be subject to the laws in force in the Australian Capital Territory, Australia.

359. This does not apply where both PKI entities to the dispute are Agencies.

360. A PKI entity may be legally represented in any mediation.

361. Nothing prevents a PKI entity from seeking urgent equitable relief before an appropriate Court.

362. Should a dispute arise between VANguard and Symantec the relevant Contract conditions apply.

9.14 Governing Law

363. This CPS, relevant CP or PDS are governed by, and are to be construed in accordance with, the laws from time to time in force in the Australian Capital Territory, Australia.

9.15 Compliance with Applicable Law

364. The PKI entities agree to submit to the jurisdiction of the courts having jurisdiction within the Australian Capital Territory, Australia.

9.16 Miscellaneous Provisions

365. A PKI entity is not liable for any loss or damage arising from any delay or failure to perform its obligations described in the CPS or the relevant CP or PDS if such delay is due to force majeure.

366. If a delay or failure by a PKI Service Provider to perform its obligations is due to force majeure, the performance of that entity's obligations is suspended.

367. If delay or failure by a PKI Service Provider to perform its obligations due to force majeure exceeds 14 days, the PKI entity affected by the failure to perform the obligations may terminate the arrangement, agreement or contract it has with the non-performing PKI Service Provider on providing notice to that PKI entity in accordance with the relevant Contract or relevant CP or PDS.

368. If the arrangement, agreement or contract is terminated, then costs shall be handled in accordance with the relevant contract or relevant CP or PDS.

9.16.1 Entire Agreement

369. To the extent of any conflict between the following documents the first mentioned document shall govern:
    - the contract between VANguard and PKI entities
    - the relevant CP or PDS and this CPS
    - another approved document.

9.16.2 Assignment

370. See the relevant CP or PDS.

9.16.3 Severability

371. Any severance of a particular provision does not affect the other provisions of this CPS, relevant CP or PDS.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

372. See the MOU and SLA entered into between VANguard and a subscriber.

9.16.5 Force Majeure

373. See the relevant PDS and the MOU and SLA entered into between VANguard and a subscriber.

9.17 Other Provisions

374. No stipulation.