# VANguard Agency Certificate Policy (CP)

## 1 Introduction

1. This document, the *VANguard Agency Certificate Policy (CP)*, sets out the rules regarding the applicability of a certificate to a particular Agency, and contains information about the specific structure of the certificate.

2. The headings of this CP 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://www.ietf.org/rfc/rfc3647.txt).

3. This document should be read in conjunction with:
   - the *VANguard Certification Practice Statement* (CPS) which describes the practices employed by the VANguard PKI in the issuance and management of digital certificates
   - the *VANguard Agency PKI Disclosure Statement* (PDS) which sets out the rules regarding the applicability of the Agency certificate, and contains information about the specific structure of the certificate
   - the *VANguard Organisational Certificate Authority (OCA) CP* which details information specific to the VANguard OCA certificates including certificates issued to Agencies.

4. The *VANguard OCA CP* is available on request. The *VANguard CPS* and the *VANguard Agency PDS* documents are publicly available online from the VANguard website: http://www.vanguard.business.gov.au

5. A document hierarchy applies:
   - the provisions of the Service Level Agreement (SLA), or other relevant contract, override the provisions of this CP
   - the provisions of the Agency PDS, and this CP, override over the provisions of the *VANguard CPS* to the extent of any direct inconsistency.

### 1.1 Overview

6. The Certificate Authority (CA) that issues the VANguard Agency certificates under this CP is the VANguard Organisational Certificate Authority (OCA).

7. VANguard Agency certificates may be used for:
   - VANguard to identify which Agency it was that submitted a transaction request
   - signing SAML authentication requests (generated by an Agency)
   - Agency client SSL authentication when accessing VANguard web services (for document time stamping and to validate document signatures)
   - Agency-to-Agency communications outside the VANguard system.

### 1.2 Document Name and Identification

8. This document is known as the VANguard Agency CP.

9. The OID for this document is: **1.2.36.1.1001.30.8.1** and is based on the following structure:

| | |
|---|---|
| 1 | ISO |
| 2 | Member Body |
| 36 | Australia |
| 1 | Government |
| 1001 | VANguard |
| 30/40/50 | Business system (VANguard Production environment) |
| 4/11 | Identifies individual object, document etc. |
| 1 | Object or document version number, incrementing from 1 |

## 1.3 PKI Participants

10. The PKI participants this CP applies to are:
    - Agencies who subscribe to VANguard services, for example Australian, State, and Local Governments
    - relying parties
    - the VANguard PKI.

### 1.3.1 Certificate Authorities (CAs)

11. The VANguard OCA will issue VANguard Agency certificates under this CP.

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

### 1.3.2 Registration Authorities (RAs)

13. VANguard provides an in-person visit by a Roaming Registration Authority (RRA) to register Agencies on site.

14. The RRA will check the following:
    - evidence of identity (EOI)
    - evidence of prior VANguard authentication.

15. The RRA will issue the Agency with their Agency keys and certificates, as well as any other VANguard trust point certificates and public keys needed to use VANguard services.

### 1.3.3 Subscribers

16. As subscribers to VANguard, Agencies must:
    - enter into and comply with the VANguard Memorandum of Understanding (MOU) and SLA
    - protect their token containing their VANguard keys and certificates from compromise
    - immediately notify VANguard if they suspect their token has, or may have been, compromised

- accept sole responsibility for the contents of any transmission, message, or other document signed using their keys and certificates
- return their token to VANguard on request
- destroy all copies of the key(s) held on the token on request
- use their keys and certificates at their sole risk
- provide accurate and complete information VANguard when applying for keys and certificates, and at all other times
- promptly notify VANguard in the event that any part of that information changes
- only use VANguard keys and certificates for the purposes authorised and not for any other purpose including for any unlawful or improper purpose
- conduct their own independent risk assessment when using VANguard certificates in non-VANguard applications, eg in Agency-to-Agency communications.

#### 1.3.4 Relying Parties

17. Relying parties may be VANguard or other parties, including other VANguard participating Agencies, who elect to use VANguard Agency Certificates in non-VANguard communications.

18. Relying parties, including other VANguard participating Agencies, are advised that before using VANguard Agency certificates to engage in Agency-to-Agency communications they should conduct their own individual risk assessment. Factors to consider are EOI processes in use, and any approvals that may have been granted by the Gatekeeper Competent Authority. In particular, Agencies are advised that it may be prudent to use the telephone or other external channel to confirm that the certificate in question is suitable for use by a particular application. See *Section 9 Other Business and Legal Matters*.

#### 1.3.5 Other Participants

19. In some situations Agency staff may participate in the VANguard PKI by fulfilling administrative roles in the management of Agency certificates. Roles involved in the administration of Agency keys are:
    - Agency Business Manager (ABM) – authorisation of actions and delegations
    - Agency Certificate Manager (ACM) – key custodians, responsible for key maintenance and management
    - Delegated RA (DRA) – for large Agencies that require the ability to manage their own certificates. The DRA generates keys and manages Agency certificates for a specific Agency (for example revocation).

### 1.4 Certificate Usage

#### 1.4.1 Appropriate Certificate Uses

20. The appropriate certificate uses are defined in this CP, and in the MOU and SLA entered into between VANguard and the subscriber.

#### 1.4.2 Prohibited Certificate Uses

21. Prohibited certificate uses are defined in the PDS and SLA entered into between VANguard and the subscriber. The User Notice in each certificate states:
*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

22. The organisation administering this document is the Department of Industry and Science (the Department), VANguard Program.

#### 1.5.2 Contact Person

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

#### 1.5.3 CPS Approval Procedures

24. The Policy Approval Authority (PAA) is responsible for governance of the PKI. Currently this function is performed by the General Manager, VANguard Program, who is responsible for all policy approval and management functions.

## 2 Publication and Repository Responsibilities

25. 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).

26. VANguard is responsible for the management of the VANguard website which publishes certificate information: http://www.vanguard.business.gov.au

27. Publication and repository responsibilities are detailed in the *VANguard CPS*.

## 3 Identification and Authentication

### 3.1 Naming

28. The Agency ABN will not be included as part of the X.500 name field, but will be present in the certificate in a custom extension field.

29. The Department authorises the use of any departmental trademark or other departmental intellectual property that may be used within Agency Certificates. Agencies consent to the use of trademarks or any other of their intellectual property appearing in the subject name field or any extensions.

30. Refer to the *VANguard CPS* for further information on naming.

### 3.2 Initial Identity Validation

31. Agency keys are generated by a VANguard RRA, in the presence of the Agency Certificate Manager. This will only be done after the RRA has been presented with satisfactory EOI, evidence of authority, and evidence of prior VANguard authentication.

32. In some cases a group of agencies (for example a number of local councils) may decide to combine and outsource the certificate management. In this case, the binding between a Business Manager in each of the agencies and a Certificate Manager in the outsourcing organisation must be documented and verified.

33. Refer to the *VANguard CPS* and the *VANguard Customer Engagement and Integration Procedure* for further information on initial identity validation.

#### 3.2.1 Method to Prove Possession of Private Key

34. Refer to the *VANguard CPS*.

#### 3.2.2 Authentication of Organisation Identity

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

#### 3.2.3 Authentication of Individual Identity

36. Each Agency identifies the individuals that represent it.

#### 3.2.4 Non-verified Subscriber Information

37. Not applicable.

#### 3.2.5 Validation of Authority

38. Each Agency identifies the individuals that represent it.

#### 3.2.6 Criteria for Interoperation

39. Not applicable.

### 3.3 Identification and Authentication for Re-key Requests

#### 3.3.1 Identification and Authentication for Routine Re-key

40. Certificates will not be re-keyed.

#### 3.3.2 Identification and Authentication for Re-key After Revocation

41. Rekey is not permitted after certificate revocation.

### 3.4 Identification and Authentication for Revocation Request

42. Agency certificates have a lifetime of four years. When these certificates approach expiry, new keys and certificates will be provided to each Agency. These new keys and certificates can be installed alongside the current ones in the Agency's certificate store.

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

44. Agency staff can only revoke their certificates by contacting the RRA and confirming their identity. This is done by having the Agency staff member answer a series of questions, such as providing the name and details of the Agency Business Manager or Agency Certificate Manager.

45. The RRA then logs into their CA account to request that the certificate is to be revoked. Once revoked, the RRA deletes the key details from the list of valid trust points held by VANguard.

# 4 Certificate Life-Cycle Operational Requirements

## 4.1 Certificate Application

### 4.1.1 Who can Submit a Certificate Application?

46. A wide range of Agencies including Australian, State and Local governments may apply for VANguard Agency certificates. The Agency must sign an MOU and enter into an SLA with VANguard.

### 4.1.2 Enrolment Process and Responsibilities

47. An RRA will be used initially. This person will have an online connection to the RA (VSP) using the Internet. The RRA checks the:
    - evidence of authentication (100 points of EOI including photo identification)
    - evidence of authority (original Authorisation Letter provided to them by the Agency Certificate Manager).

48. The VANguard Business Manager is responsible for checking the paperwork for accuracy and enters these details into the system:
    - Agency ID, MoU
    - Business Manager, authority
    - Certificate Manager, authority
    - Request authority
    - Contact phone numbers.

49. The Agency is responsible for ensuring all information provided is complete, accurate, and up-to-date.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

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

### 4.2.2 Approval or Rejection of Certificate Applications

51. 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

52. 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

53. The VANguard CA, when issuing a certificate, will ensure at the time it issues a certificate that:
    - the VANguard 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 this CP and Agency PDS.

#### 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

54. Refer to the *VANguard CPS*.

### 4.4 Certificate Acceptance

#### 4.4.1 Conduct Constituting Certificate Acceptance

55. Certificate acceptance is either:

- the signed 'Confirmation of Receipt and Acceptance of Certificates and Keys' (RRA) form, or
- the use of the VANguard Agency keys and certificate.

56. For further information, refer to the *VANguard CPS*.

#### 4.4.2 Publication of the Certificate by the CA

57. Refer to the *VANguard CPS*.

#### 4.4.3 Notification of Certificate Issuance by the CA to other Entities

58. Refer to the *VANguard CPS*.

### 4.5 Key Pair and Certificate Usage

#### 4.5.1 Subscriber Private Key and Certificate Usage

59. Use is restricted according to the terms of the SLA and the *VANguard Agency PDS*.

60. There is no obligation to provide any particular functionality, and the supported applications may change over time.

#### 4.5.2 Relying Party Public Key and Certificate Usage

61. Relying parties using a VANguard Agency certificate must check the certificate chain up to the issuing CA and check the applicable CRL at: http://crl.verisign.com.au//DepartmentofInnovationIndustryScienceandResearchAustralianAuthenticationandNotaryServicesAgency/LatestCRL.crl

62. A relying party must promptly notify VANguard in the event that it suspects that there has been a compromise of the relevant private keys.

### 4.6 Certificate Renewal

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

### 4.7 Certificate Re-key

#### 4.7.1 Circumstance for Certificate Re-key

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

### 4.8 Certificate Modification

#### 4.8.1 Circumstance for Certificate Modification

65. Certificates will not be modified; instead they will be reissued before certificate expiry.

### 4.9 Certificate Revocation and Suspension

66. Refer to the *VANguard CPS* for detailed information on certificate revocation and suspension.

#### 4.9.1 Circumstances for Revocation

67. An Agency certificate would be immediately revoked in the case of compromise. Revocation would also occur in the event of PKI termination.

68. The RA reserves the right to revoke any certificate at any time and for any reason.

#### 4.9.2 Who Can Request Revocation

69. Revocation of an Agency certificate can be requested by any Agency or other party who suspects compromise.

#### 4.9.3 Procedure for Revocation Request

70. Agency staff can only revoke their certificates by contacting the RRA and confirming their identity. This is done by having the Agency staff member answer a series of questions, such as providing the name and details of the Agency Business Manager or Agency Certificate Manager.

### 4.10 Certificate Status Services

71. Refer to the *VANguard CPS*.

### 4.11 End of Subscription

72. No stipulation.

### 4.12 Key Escrow and Recovery

73. Agency private keys are not escrowed.

## 5 Facility, Management, and Operational Controls

74. Refer to the *VANguard CPS* which 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.

## 6 Technical Security Controls

### 6.1 Key Pair Generation and Installation

75. Comprehensive information on all keys is contained in three separate documents: the *VANguard CPS*, the *VANguard Key Register*, and the *VANguard Key Management Plan*.

76. This CP only deals with the Agency certificate keys.

#### 6.1.1 Key Pair Generation

77. Keys for subscribers are generated by the RA.

78. Key pair generation is performed in accordance with the KMP.

### 6.1.2 Private Key Delivery to Subscriber

79. Following key generation, the RRA exports the Agency's key pair to a P#12 file encrypted using a password created and entered by the Agency Certificate Manager. The RRA then burns the P#12 file to two identical CD ROMs.

### 6.1.3 Public Key Delivery to Certificate Issuer

80. See *Section 4.3 Certificate Issuance*.

### 6.1.4 CA Public Key Delivery to Relying Parties

- These will distributed directly to Agencies by the VANguard RRA in person as part of initial enrolment, or
- The VANguard CA's public key, or the public keys of subordinate CAs, is delivered to a subscriber in an online transfer which meets the *Internet Engineering Task Force Request for Comment* 4210 - *Internet X.509 Public Key Infrastructure Certificate Management Protocols* (http://www.ietf.org/rfc/rfc4210.txt) standard, or
- The VANguard RCA public key, and the public keys of all subordinate CAs, are available to download from the repository.

### 6.1.5 Key Sizes

81. Agency certificate key lengths are 1024 bits.

82. Agency keys are generated using the RSA algorithm. The RSA algorithm does not require the generation of parameters.

83. Keys may only be used in compliance with this CP, and all restrictions described in this CP must be observed. The 'Key Usage' field provides an indication of acceptable usage, regardless of whether this field is technically used by an application. While this extension is designated as non-critical it does not indicate any reduced need for compliance.

### 6.1.6 Public Key parameters Generation and Quality Checking

84. 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)

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

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

86. Refer to the *VANguard CPS.*

## 6.3 Other Aspects of Key Pair Management

87. Refer to the *VANguard CPS.*

## 6.4 Activation Data

88. Refer to the *VANguard CPS.*

## 6.5 Computer Security Controls

89. Refer to the *VANguard CPS.*

### 6.6 Life Cycle Technical Controls

90. Refer to the *VANguard CPS.*

### 6.7 Network Security Controls

91. Refer to the *VANguard CPS.*

### 6.8 Time-Stamping

92. Refer to the *VANguard CPS.*

## 7 Certificate, CRL, and OCSP Profiles

### 7.1 Certificate Profile

93. This section contains the Agency certificate profile for the VANguard PKI.

94. For further information refer to the *VANguard CPS* and the *VANguard Agency PDS*.

95. Agency Certificate Attributes are as follows:

| **Attribute** | **Value** |
|---|---|
| Issuer Name | cn=Australian Government Notary Services OCA<br>ou=Australian Authentication and Notary Services<br>o=Australian Government<br>c=AU |
| Subject Name | cn=<*Provided by Agency*><br>ou=<*Optional field provided by Agency*><br>o=<*Agency Name*><br>c=AU |
| Signature Algorithm | SHA1 with RSA encryption |
| RSA Public Key | 1024 bits |
| Certificate Validity | 4 years |
| Certificate Renewal | Recommended 3 years and 6 months |

96. Agency certificate extensions are as follows:

| **Extension** | **Extension Value/Contents** |
|---|---|
| CRL Distribution Point | http://crl.verisign.com.au//DepartmentofInnovationIndustryScienceandResearchAustralianAuthenticationandNotaryServicesAgency/LatestCRL.crl |
| Key Usage | Digital Signature, Non Repudiation, Key Encipherment, Key Agreement |
| Subject Key Identifier | The identifier will change for every Agency certificate that is generated. All Subject Key Identifiers are unique. |
| Authority Key Identifier | keyid:5F:2B:FC:D9:35:A7:11:41:0C:30:06:D0:6F:74:B8:D3:7B:91:8D:C3 |

| Extension | Extension Value/Contents |
|---|---|
| Certificate Policies | OID:<br>1.2.36.1.1001.30.8.1<br>CPS URL:<br>http://www.agns.business.gov.au<br>UserNotice: ExplicitText:<br>*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.* |
| Basic Constraints | CA Boolean = False |
| ABN custom extension | Identified by the ABN-DSC custom certificate extension OID 1.2.36.1.333.1<br>Contains the ABN value of the Agency. |

### 7.1.1 Version Number(s)

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

### 7.1.2 Certificate Extensions

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

### 7.1.3 Algorithm Object Identifiers

99. The VANguard PKI uses only those cryptographic algorithms approved by the Australian Signals Directorate (DSD).

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

### 7.1.4 Name Forms

101. Certificates issued under this CP contain the full Distinguished Name of the CA issuing the certificate in the 'Issuer Name' field of the certificate profile.

### 7.1.5 Name Constraints

102. Anonymous or pseudonymous names are not supported.

### 7.1.6 Certificate Policy Object Identifier

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

104. This field contains the policy OID: 1.2.36.1.1001.30.8.1

105. See *Section 1.2* for details on how the OID is constructed.

### 7.1.7 Usage of Policy Constraints Extension

106. Not applicable.

### 7.1.8 Policy Qualifiers Syntax and Semantics

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

108. The certificate policies extension is used to clearly indicate the policy under which the Agency certificate has been issued, and the purposes for which the certificates may be used. The userNotice explicitText field reads as follows:
*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.*

#### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

109. This extension is used, but set to non-critical. However, the provisions of this CP should be complied with.

110. This X.509 CP complies with the Australian standard X.509 profile.

### 7.2 CRL Profile

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

| Attribute | Value |
|---|---|
| CRL Distribution Point | http://crl.verisign.com.au//DepartmentofInnovationIndustryScienceandResearchAustralianAuthenticationandNotaryServicesAgency/LatestCRL.crl |
| CRL validity | 24 hours (from 12am each day) |
| CRL signature digest | SHA-1 |

#### 7.2.1 Version Number(s)

112. The VANguard PKI supports and uses X.509 v1 CRLs.

#### 7.2.2 CRL and CRL Entry Extensions

113. The VANguard PKI supports and uses X.509 v1 CRL entry extensions as indicated in the CRL profile.

### 7.3 OCSP Profile

114. Not applicable.

115. Refer to the *VANguard CPS*.

## 8 Compliance Audit and Other Assessments

116. VANguard's Gatekeeper accredited certificate provider (Symantec) is accountable to the Gatekeeper Competent Authority for their compliance with relevant standards and the Gatekeeper regime overall.

117. VANguard may be subject to an audit by the Privacy Commissioner and the Commonwealth or State Auditor-General(s).

118. VANguard will conduct an Infosec - Registered Assessor Program (IRAP) assessment against the requirements of the *Australian Government Information Security Manual* (ISM), or any replacement manual, and the *Protective Security Policy Framework* (PSPF), or any replacement manual.

119. Refer to the *VANguard CPS* for further information on compliance audits and other assessments.

# 9 Other Business and Legal Matters

120. This section contains default provisions that may be overridden by the provisions of an applicable contract. Generally, Agencies using VANguard services must sign an SLA. If both the SLA and the CP are silent on an issue, the default provisions of the *VANguard CPS* apply.

## 9.1 Fees

121. VANguard does not currently charge fees for Agency certificates or use of VANguard services where the Agency uses services without modification and without having significant impact on the VANguard system capacity or performance.

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

## 9.2 Financial Responsibility

123. See the relevant SLA in relation to Agencies or other applicable contract in the case of other business relationships such as with service providers.

## 9.3 Confidentiality of Business Information

124. VANguard may not disclose the confidential information of an Agency, or use that information for any purpose, except:
    - to its staff requiring the information for the purposes of this agreement or for delivery of the services
    - with the consent of the Agency
    - if required to do so by any law, or
    - to the extent necessary in connection with legal proceedings relating to an applicable agreement.

125. Notwithstanding the above clause, VANguard may disclose confidential information of the Agency if required or requested to do so by a House of the Commonwealth Parliament, or a Commonwealth Parliamentary Committee. Where practicable VANguard will give prior notice to the Agency of any disclosure under this clause.

### 9.3.1 Scope of Confidential Information

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

127. See the MOU and SLA between VANguard and the subscriber for information not within the scope of confidential information, and the responsibility to protect that information.

## 9.4 Privacy of Personal Information

128. Agency certificates will contain the Agency name and Australian Business Number (ABN). The Agency certificates subject to this CP contain no personal information. All VANguard certificate policies and practices require strict adherence to the *Privacy Act 1988 (Cth*) including, as appropriate, the Information Privacy Principles and the National Privacy Principles.

## 9.5 Intellectual Property Rights

129. Refer to the *VANguard CPS*.

## 9.6 Representations and Warranties

### 9.6.1 CA Representations and Warranties

130. Refer to the *VANguard CPS*.

### 9.6.2 RA Representations and Warranties

131. Refer to the *VANguard CPS*.

### 9.6.3 Subscriber Representations and Warranties

132. The rights and obligations of Agencies are defined in the applicable SLA. Agencies cannot provide any warranties in respect of the operations of the VANguard PKI but are responsible for the safeguarding and appropriate use of their keys and certificates.

### 9.6.4 Relying Party Representations and Warranties

133. Any party seeking to rely, without having entered into a separate written agreement with VANguard, must comply with obligations and restrictions set out in this CP. No reliance for financial transactions is supported.

### 9.6.5 Representations and Warranties of Other Participants

134. The information in the certificate is true to the best of the CA's knowledge after performing certain identity authentication procedures with due diligence.

135. No implied or express warranties are given by the Department, or by any other entity, either in Subscriber or Relying Party Agreements.

## 9.7 Disclaimers of Warranties

136. 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.

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

## 9.8 Limitations of Liability

138. In the absence of any separate contractual assumption of liability to an Agency or other party, the Department does not accept any liability regarding the operations of the VANguard PKI, including the use of or reliance upon VANguard Agency certificates.

## 9.9 Indemnities

139. Unless otherwise set forth in contract, all subscribers and relying parties continually indemnify the Department from and against any or all losses, damages, liabilities, claims or expenses (including reasonable solicitor-client costs) incurred or suffered by the Department as a result of any act or omission in relation to the issuing, use or management of VANguard keys and certificates, or any other subject matter provided for under this CP.

## 9.10 Term and Termination

### 9.10.1 Term

140. This CP remains in force until replaced by a new version of this CP or until termination is indicated on the VANguard website: http://www.vanguard.business.gov.au

141. The provisions of this CP remain in effect until the expiry or revocation of the last issued certificate if not terminated sooner.

### 9.10.2 Termination

142. This document terminates upon release of a new version of the CP or upon termination of operations of the CA or PKI.

### 9.10.3 Effect of Termination and Survival

143. Indemnities, intellectual property, and confidentiality clauses shall survive termination of this CP.

## 9.11 Individual Notices and Communications with Participants

144. Communication with Agencies will be as per the relevant SLA.

## 9.12 Amendments

### 9.12.1 Procedure for Amendment

145. Changes that do not materially affect use of certificates issued under this CP may be made at the discretion of authorised VANguard employees. Such changes do not require notice to be given to any party and do not require a new OID to be allocated. Changes that do not materially affect use include editorial corrections, typographical corrections, changes to contact details and any other change deemed to have no effect on the level of assurance or acceptability of related certificates.

### 9.12.2 Notification Mechanism and Period

146. Refer to the *VANguard CPS*.

### 9.12.3 Circumstances under Which OID Must be Changed

147. The OID must be changed if there has been a change in policy that materially affects subscribers, relying parties or other participants. A material change includes any change deemed to affect the reliance, level of assurance or acceptability of an existing certificate class. Material changes require the consent of the VANguard PAA.

## 9.13 Dispute Resolution Procedures

148. Any party may give another a notice of dispute under this CP. The parties will use all reasonable endeavours to resolve any dispute notified under this clause promptly, initially by discussions between the VANguard Representative and the Agency Representative, and including by escalation where appropriate.

149. Nothing in this clause affects any party's rights or its ability to commence legal proceedings.

## 9.14 Governing Law

150. The law of the Australian Capital Territory shall govern the interpretation and enforcement of this CP and any associated documents and agreements.

## 9.15 Compliance with Applicable Law

151. This CP requires all participants to comply with the applicable law.

## 9.16 Miscellaneous Provisions

152. Refer to the *VANguard CPS*.

### 9.16.1 Entire Agreement

153. This CP is complemented by:

- the *VANguard CPS* which describes the practices used by the CA in issuing and managing certificates, and
- a contract between the Department and the user of the VANguard services.

154. The terms and conditions of the contract will override the provisions of this CP and the *VANguard Agency* PDS, and the provisions of the CP and the *VANguard Agency PDS* will override the provisions of the *VANguard CPS*. The *VANguard CPS* provides default provisions to take effect when the other documents are silent on the matter in question.

### 9.16.2 Assignment

155. The Agency may not assign any of its rights or obligations in relation to the use of VANguard services and certificates without the prior consent of the Department.

### 9.16.3 Severability

156. If any provision of this CP is held to be invalid, illegal or unenforceable, such provision will be severed and the remainder of the provisions will remain in full force and effect.

### 9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

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

### 9.16.5 Force Majeure

158. No party is in breach of this CP for any act, omission or failure to fulfil its obligations under this CP if such act, omission or failure arises from any cause reasonably beyond its control (force majeure).

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

## 9.17 Other Provisions

160. No stipulation.