Australian Government
Department of Industry, Innovation and Science

VANguard Agency Certificate Policy (CP)

Vdoc507

Version 1.0

December 2018

Contents

1. Introduction

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

VANguard Agency certificates are also referred to as “Client” or “Relying Party” certificates.

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 (PKI) Certificate Policy and Certification Practices Framework.

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 Relying Party PKI Disclosure Statement (PDS) which sets out the rules regarding the applicability of the relying party 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 relying parties.

The VANguard OCA CP is available on request. The VANguard CPS and the VANguard Relying Party PDS documents are publicly available online from the Department of Industry, Innovation and Science website.

A document hierarchy applies:

- the provisions of VANguard’s governance arrangements, or other relevant contract/s, override the provisions of this CP
- the provisions of the PDS, and the CPS, override the provisions of the VANguard Relying Party CP to the extent of any direct inconsistency.

1.1 Overview

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

VANguard relying party certificates may be used for:

- VANguard to identify which relying party it was that submitted a transaction request
- signing SAML authentication requests (generated by a relying party)
- relying party client SSL authentication when accessing VANguard web services (for document time stamping and to validate document signatures)

- communications outside the VANguard system.

1.2 Document Name and Identification

This document is known as the VANguard Relying Party CP.

The OID for this document is: 1.2.36.1.1001.30.8.2 and is based on the following structure:

1	ISO
2	Member Body
36	Australia
1	Government
1001	VANguard
30, 40, or 50	Business system (VANguard Production environment is 30)
4 - 11	Identifies individual object, document etc. (Relying Party Certificate is 8)
2	Object or document version number, incrementing from 1

1.3 PKI Participants

The PKI participants this CP applies to are:

- Clients who subscribe to VANguard services, for example Australian, State, and Local Governments or commercial software providers who provide Federated Authentication Service-enabled applications
- relying parties
- the VANguard Managed Public Key Infrastructure (MPKI).

1.3.1 Certificate Authorities (CAs)

The VANguard OCA will issue VANguard relying party certificates under this CP.

Certificate services, including CA management and operations for VANguard, are provided using the DigiCert Gatekeeper accredited MPKI.

1.3.2 Registration Authorities (RAs)

Where possible, VANguard provides an in-person visit by a Roaming Registration Authority (RRA) to register Clients on site. In some circumstances a Registration Authority can complete the registration remotely. These circumstances include excessive travel costs.

The RA will check the following:

- evidence of identity (EOI)
- evidence of authority (EOA) to act on behalf of an organisation
- evidence of prior VANguard authentication.

The RA will enrol the relying party for the certificates using the email address nominated by the Certificate Manager. This generates an enrolment code that the RA provides securely to the Certificate Manager. The RA then approves the enrolment request which issues a certificate download link to the nominated account. This link in conjunction with the enrolment enables the Certificate Manager to download the certificate.

The RA will also provide the relying party with any other VANguard trust point certificates and public keys needed to use VANguard services.

1.3.3 Subscribers

As subscribers to VANguard, Clients must:

- enter into and comply with the VANguard governance arrangements
- protect their VANguard issued keys and certificates from compromise
- immediately notify VANguard if they suspect their keys or certificates have, or may have been, compromised
- accept sole responsibility for the contents of any transmission, message, or other document signed using their keys and certificates
- destroy all copies of the key(s) on request
- use their keys and certificates at their sole risk
- provide accurate and complete information to 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.

1.3.4 Relying Parties

Relying parties may be participating Agencies or organisations, who elect to use VANguard relying party certificates in non-VANguard communications.

Relying parties, including other VANguard participating Agencies, are advised that before using VANguard relying party certificates to engage in other 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, relying parties 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

In some situations relying party staff may participate in the VANguard MPKI by fulfilling administrative roles in the management of relying party certificates. Roles involved in the administration of relying party keys are:

- Business Manager (BM) – authorisation of actions and delegations
- Certificate Manager (CM) – key custodians, responsible for key maintenance and management

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The appropriate certificate uses are defined in this CP.

1.4.2 Prohibited Certificate Uses

Prohibited certificate uses are defined in the PDS.

The User Notice in each certificate states:

This certificate is subject to the usage constraints and limitations of liability contained in the PDS. Reliance not expressly permitted in those documents is not supported.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

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

1.5.2 Contact Person

If you have any questions in relation to this CP email the VANguard team VANguard.Customer@industry.gov.au

1.5.3 CPS Approval Procedures

The Policy Approval Authority (PAA) is responsible for governance of the MPKI. 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

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

Publication and repository responsibilities are detailed in the VANguard CPS which can be found on Department of Industry, Innovation and Science website.

3. Identification and Authentication

3.1 Naming

The relying party 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.

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

Refer to the VANguard CPS for further information on naming.

3.2 Initial Identity Validation

Keys are generated by the client and approved by a VANguard RA, preferably in the presence of the Certificate Manager. This will only be done after the RA has been presented with satisfactory EOI, EOA, and evidence of prior to approval.

In some cases a group of clients (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.

Refer to the VANguard CPS and the VANguard Client Engagement and Integration Process for further information on initial identity validation.

3.2.1 Method to Prove Possession of Private Key

Refer to the VANguard CPS.

3.2.2 Authentication of Organisation Identity

Refer to the VANguard Client Engagement and Integration Process.

3.2.3 Authentication of Individual Identity

Authentication occurs through the production of identity production according to the National Identity Proofing Guidelines to the 100 point level.

3.2.4 Non-verified Subscriber Information

Not applicable.

3.2.5 Validation of Authority

Each relying party nominates the individuals that represent it as part of the VANguard Client Engagement and Integration Process.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Certificates will not be re-keyed.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key is not permitted after certificate revocation.

3.4 Identification and Authentication for Revocation Request

Relying party certificates normally have a lifetime of four years. When these certificates have been compromised or for some other reason need to the revoked, prior to expiry, VANguard will handle the revocation and de-provisioning of the certificate in question.

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

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

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?

A wide range of Agencies including Australian, State and Local governments as well as commercial entities providing services to government, may apply for VANguard relying party certificates. The relying party may sign an MOU and must enter into an SLA with VANguard.

4.1.2 Enrolment Process and Responsibilities

An RRA will be used initially. This person will have an online connection to the RA Website over the Internet. The RRA checks the:

- evidence of identity (100 points of EOI including photo identification in accordance with the National Identity Proofing Guidelines)
- evidence of authority (original Authorisation Letter for each Certificate Manager signed by the Business Manager).

Where an RA needs to complete the process remotely, the evidence of identity (100 points of EOI including photo identification) must be signed by a Justice of the Peace (JP), and submitted to VANguard by the individual from an email account associated with their organisation.

The VANguard Business Manager is responsible for checking the paperwork for accuracy and enters these details into the system:

- relying party ID
- Business Manager, authority
- Certificate Manager, authority
- request authority
- contact phone numbers.

The relying party is responsible for ensuring all information provided is complete, accurate, and up-to-date, and is also responsible for updating VANguard of any changes as soon as practicable after they occur.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

4.2.2 Approval or Rejection of Certificate Applications

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

The Certificate Application Process will vary in time depending on whether a client is a new client or existing. For new clients, certificate issue is timed in accordance with the onboarding process.

For Certificate renewals, processing is within 3 business days provided the client has presented the relevant documentation for Evidence of Identity.

For cases where compromised or lost credentials require expedited service, the VANguard Client Team will make best efforts to re-issue during business hours in accordance with the defined processes.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

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 the VANguard Relying Party PDS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Refer to the VANguard CPS.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Certificate acceptance is both:

- the signed 'Certificate Acceptance' form, and
- verification by the Client Engagement team that the certificate has been downloaded.

For further information, refer to the VANguard CPS.

4.4.2 Publication of the Certificate by the CA

Refer to the VANguard CPS.

4.4.3 Notification of Certificate Issuance by the CA to other Entities

Refer to the VANguard CPS.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use is restricted according to the terms of the SLA and the VANguard Relying Party PDS.

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

Relying parties using a VANguard relying party certificate must check the certificate chain up to the issuing CA and check the applicable CRL at:

http://pki-crl.symauth.com/ca_30120b672b776150513b8147f6592778/LatestCRL.crl

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

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

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

Certificates will not be modified; instead they will be reissued with the appropriate changes.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

A relying party certificate would be immediately revoked in the case of compromise. Revocation would also occur in the event of MPKI termination.

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

4.9.2 Who Can Request Revocation

Revocation of a certificate can be requested by any relying party or other party who suspects compromise.

4.9.3 Procedure for Revocation Request

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

4.10 Certificate Status Services

Refer to the VANguard CPS.

4.11. End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

Relying party private keys are not escrowed.

5. Facility, Management, and Operational Controls

Refer to the VANguard CPS which details the controls in place at the DigiCert 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

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

This CP only deals with the relying party certificate keys.

6.1.1 Key Pair Generation

Keypair Generation occurs in the user's browser as part of the certificate issuance process.

6.1.2 Private Key Delivery to Subscriber

The private key is generated in the user's browser in the user's environment. There is no key delivery step. The public key is sent to the CA and incorporated into the user's certificate and returned as part of the issuance process.

6.1.3 Public Key Delivery to Certificate Issuer

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 key of the OCA, are available to download from the repository.

6.1.5 Key Sizes

Relying party certificate key lengths are 2048 bits.

Relying party keys are generated using the RSA algorithm. The RSA algorithm does not require the generation of parameters.

6.1.6 Public Key parameters Generation and Quality Checking

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)

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.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Refer to the VANguard CPS.

6.3 Other Aspects of Key Pair Management

Refer to the VANguard CPS.

6.4 Activation Data

Refer to the VANguard CPS.

6.5 Computer Security Controls

Refer to the VANguard CPS.

6.7 Life Cycle Technical Controls

Refer to the VANguard CPS.

6.8 Network Security Controls

Refer to the VANguard CPS.

6.9 Time-Stamping

Refer to the VANguard CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

This section contains the relying party certificate profile for the VANguard PKI.

For further information refer to the VANguard CPS and the VANguard Relying Party PDS.

Certificate attributes are as follows:

Attribute	**Value**
Issuer Name	cn=Australian Government Notary Services OCA ou=Australian Authentication and Notary Services o=Australian Government c=AU

Subject Name	cn=<*Provided by relying party*> ou=<*Optional field provided by relying party*> o=<*Relying Party Name*> c=AU
Signature Algorithm	SHA256 with RSA encryption
RSA Public Key	2048 bits
Certificate Validity	4 years
Certificate Renewal	Recommended 3 years and 6 months

Certificate extensions are as follows:

Extension	**Extension Value/Contents**
CRL Distribution Point	http://pki-crl.symauth.com/ca_30120b672b776150513b8147f6592778/LatestCRL.crl
Key Usage	Digital Signature, Non Repudiation, Key Encipherment, Key Agreement
Subject Key Identifier	The identifier will change for every 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
Certificate Policies	OID: 1.2.36.1.1001.30.8.1 CPS URL: http://www.agns.business.gov.au UserNotice: ExplicitText: *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 Contains the ABN value of the relying party.

7.1.1 Version Number(s)

The VANguard PKI supports and uses Version 3 certificates.

7.1.2 Certificate Extensions

The VANguard PKI supports and uses Version 3 certificate extensions.

7.1.3 Algorithm Object Identifiers

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

OIDs are not allocated to algorithms in the VANguard MPKI.

7.1.4 Name Forms

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

Anonymous or pseudonymous names are not supported.

7.1.6 Certificate Policy Object Identifier

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

This field contains the policy OID: 1.2.36.1.1001.30.8.2

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

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

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

The certificate policies extension is used to clearly indicate the policy under which the relying party 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

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

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

7.2 CRL Profile

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://pki-crl.symauth.com/ca_30120b672b776150513b8147f6592778/LatestCRL.crl
CRL validity	24 hours (from 12am each day)
CRL signature digest	SHA256

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

Not applicable.

Refer to the VANguard CPS.

8. Compliance Audit and Other Assessments

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

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

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.

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

9. Other Business and Legal Matters

This section contains default provisions that may be overridden by the provisions of an applicable contract or governance arrangement. Generally, Clients using VANguard services must enter into an agreement with VANguard. If both the agreement and the CP are silent on an issue, the default provisions of the VANguard CPS apply.

9.1 Fees

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

There may be costs associated where Clients wish to use certificates for their own programs.

9.2 Financial Responsibility

See the relevant governance agreement 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

VANguard may not disclose the confidential information of any relying party, 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 relying party
- if required to do so by any law, or
- to the extent necessary in connection with legal proceedings relating to an applicable agreement.

Notwithstanding the above clause, VANguard may disclose confidential information of the relying party 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 relying party of any disclosure under this clause.

9.3.1 Scope of Confidential Information

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

See the governance agreement/s 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

Certificates will contain the relying party name and Australian Business Number (ABN). The 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

Refer to the VANguard CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Refer to the VANguard CPS.

9.6.2 RA Representations and Warranties

Refer to the VANguard CPS.

9.6.3 Subscriber Representations and Warranties

The rights and obligations of relying party are defined in the applicable governance agreement/s. Clients 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

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

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

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

9.7 Disclaimers of Warranties

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.

See the relevant PDS and/or governance arrangements between VANguard and the relying party.

9.8 Limitations of Liability

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

9.9 Indemnities

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

This CP remains in force until replaced by a new version of this CP or until termination is indicated on the Department of Industry, Innovation and Science website.

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

This document terminates upon release of a new version of the CP or upon termination of operations of the OCA or MPKI.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

Communication with relying parties will be as per the relevant governance arrangements.

9.12 Amendments

9.12.1 Procedure for Amendment

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

Refer to the VANguard CPS.

9.12.3 Circumstances under Which OID Must be Changed

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

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 relying party representative, and including by escalation where appropriate.

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

9.14 Governing Law

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

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

9.16 Miscellaneous Provisions

Refer to the VANguard CPS.

9.16.1 Entire Agreement

This CP is complemented by:

- the VANguard CPS which describes the practices used by the CA in issuing and managing certificates, and
- any governance arrangement or contract between the Department and the user of the VANguard services.

The terms and conditions of the governance arrangement or contract will override the provisions of this CP and the VANguard Relying Party PDS. The VANguard CPS provides default provisions to take effect when the other documents are silent on the matter in question.

9.16.2 Assignment

The relying party 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

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)

See the governance arrangements entered into between VANguard and a subscriber.

9.16.5 Force Majeure

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).

See the governance arrangements entered into between VANguard and a subscriber.

9.17 Other Provisions

No stipulation.