Australian Government
Department of Industry, Innovation and Science

VANguard Certification Practice Statement (MPKI8)

Vdoc539

Version 1.6

November 2018

Table of Contents

1 Introduction

The Department of Industry, Innovation and Science (the Department), is responsible for managing the VANguard Program (VANguard). VANguard is a whole of government program that delivers authentication services to secure business to government (B2G) and government to government (G2G) online transactions.

VANguard uses a Public Key Infrastructure (PKI) to:

- provide independent and indisputable evidence of online B2G and G2G transactions ensuring non-repudiation (time stamping services)
- verify assertions 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 secure fraud detection, and two-factor authentication, for protecting online identities and interactions between consumers, business partners, and employees.

The DigiCert Gatekeeper accredited Managed Public Key Infrastructure (MPKI) provides the Certificate Authority (CA) management for VANguard.

VANguard uses an MPKI with a Root Certificate Authority (RCA), and one subordinate CA – the Organisational CA (OCA). The OCA issues the VANguard system certificates and public certificates to relying parties.

1.1 Overview

This Certification Practice Statement (CPS) sets out a number of policy and operational matters for issuing Gatekeeper X.509 v3 compliant certificates as defined in the Gatekeeper PKI Framework. Information describing the Gatekeeper PKI Framework can be found at the Digital Transformation Agency website. It also includes the practices that DigiCert uses in issuing, revoking, and managing VANguard certificates.

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*. However, only those headings that pertain to the VANguard are included, and the remaining headings are excluded resulting in some numbering gaps.

This CPS sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing digital certificates for the VANguard MPKI, as well as providing information on the secure management of the core infrastructure that supports the VANguard MPKI. VANguard digital certificates meet the x.509 standards and accommodate inclusion of the Australian Business Number (ABN) where appropriate.

This CPS covers only those matters specific to the VANguard certificates, including the obligations of the PKI entities, as identified in Section 1.3. The obligations of relying parties are also set out in the relevant Service Level Agreement (SLA), and the Memorandum of Understanding (MOU).

This CPS should be read in conjunction with:

- the Certificate Policy (CP) which sets out rules regarding the applicability of a certificate to a particular agency, and contain information about the specific structure of the relevant certificate type
- the PKI Disclosure Statement (PDS) that provides additional detail and further provisions for the benefit of relying parties (end entities)
- the Memorandum of Understanding (MOU) and Service Level Agreement (SLA) between VANguard and the relying party
- the contract for services between VANguard and DigiCert.

1.2 Document Name and Identification

This document is known as the 'VANguard Certification Practice Statement'.

1.3 PKI Participants

The VANguard MPKI participants include Australian, State, Territory, and Local government agencies, suppliers, contractors, and organisations. The MPKI participants are referenced in this document as relying parties.

1.3.1 Certification Authorities

As part of the VANguard Program, DigiCert provides an MPKI service that includes a private CA hierarchy of a VANguard Root CA (RCA) and one subordinate CA (VANguard OCA).

The VANguard MPKI implements the RCA to provide the trust anchor for cryptographic communications using X.509 certificates. The RCA serves as the top level root of trust for the MPKI hierarchy and as such is itself the issuer of its own certificate (it possesses a self-signed certificate). As the trust anchor, the RCA certificate is used to sign the OCA at the subordinate level of the hierarchy in accordance with the policies of this document. The RCA does not issue end-entity certificates.

Certificate Type	Certificate Issuer
VANguard RCA	Self issued
VANguard OCA	VANguard RCA

The subordinate OCA issues end entity certificates for relying parties by digitally signing and issuing end entity certificate requests that are approved by the VANguard RA.

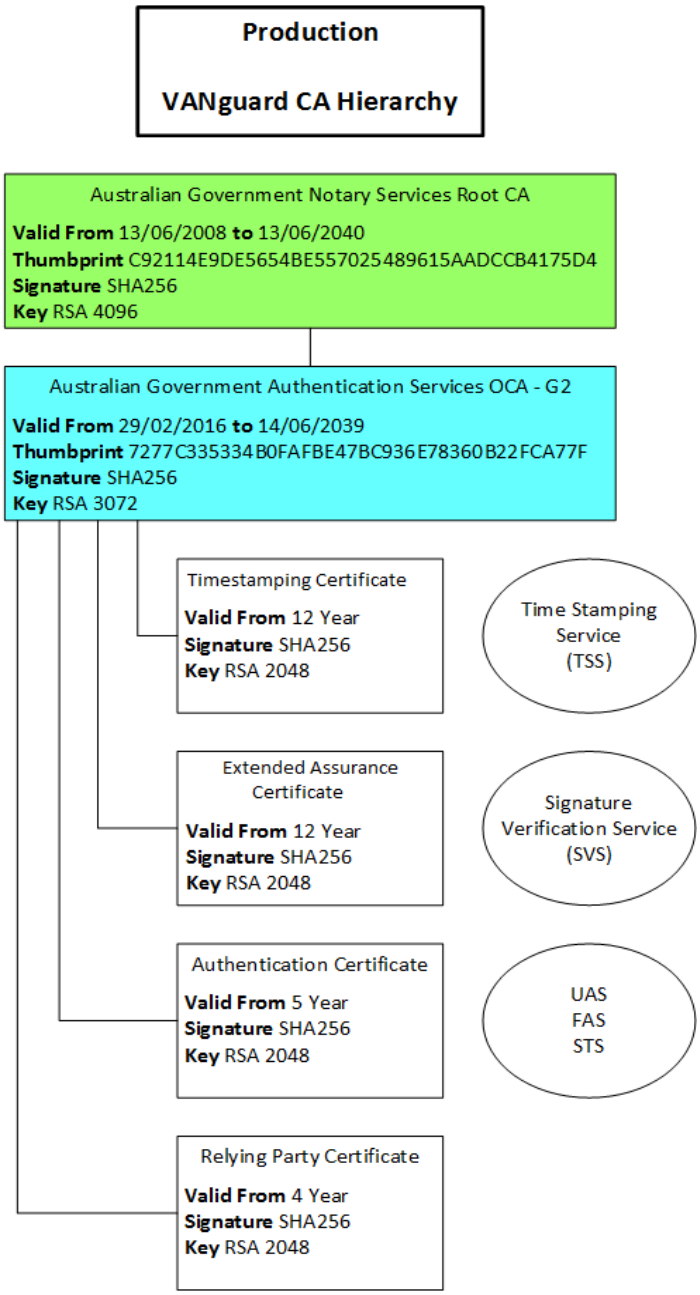
There are four (4) different types of end entity certificates available in VANguard. Each type of certificate has a unique purpose and is issued under the OCA as follows:

Certificate Type	Certificate Issuer
VANguard Relying Party Certificate	VANguard OCA
VANguard Authentication Certificate	VANguard OCA
VANguard Notary Certificate	VANguard OCA
VANguard Assertion Certificate	VANguard OCA

These are described in more detail below:

- VANguard Relying Party Certificate - these certificates are issued to (and hosted by) authorised agencies and organisations. Relying Party certificates are used to authenticate to the VANguard web services environment and to digitally sign SAML authentication requests.
- VANguard Authentication Certificate - these certificates are used to digitally sign SAML responses as well as short lived SAML assertions.
- VANguard Notary Certificate - the private keys reside on HSMs hosted within the Department, and are used for the digital time stamping of documents.
- VANguard Assertion Certificate - the private keys reside on HSMs hosted within the Department and are used to digitally sign long lived SAML assertions.

Figure 1: VANguard Managed PKI



The authorisation for issuance and renewal of a certificate is conducted by the VANguard MPKI technical team. All certificate life cycle operations are performed via controlled and audited processes, involving multiple trusted role participants within a physically protected facility as described in Sections 5 and Section 6.

1.3.2 Registration Authorities

The VANguard MPKI establishes contractual relationships with relying parties enrolled for certificate services. Certificates are issued under an Evidence of Identity (EOI) model, as determined by the Gatekeeper Framework, where all applicants undergo a face-to-face EOI check in the presence of an accredited VANguard Registration Authority (RA).

The EOI is used to identify a person as an employee or representative of an organisation. It is also used to identify a person as the Certificate Manager who is then responsible for managing the certificate on behalf of the organisation. The individuals are not named within the certificate.

The VANguard RA keys are managed by the Department using RA software provided by DigiCert. 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 End Entities

The end entities to which this CPS applies are relying parties.

1.3.3.1 Subscribers

See Section 1.3 PKI Participants.

1.3.3.2 Relying Parties

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

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

1.3.4 Other Participants

1.3.4.1 Authoriser

An authoriser appoints an individual with the relying party to fulfil the role of Certificate Manager on behalf of the organisation. Authorisers include (but are not limited to):

- Chief Executive Officer
- Company Director
- Trustee
- Partner
- Company Owner

1.3.4.2 Certificate Manager

A Certificate Manager performs delegated RA tasks for the VANguard digital certificates within the relying party.

The Certificate Manager uses a certificate for authentication to perform their duties. They accept the SLA prior to receipt of the certificate.

1.3.4.2.1 Responsibilities in Certificate Issuance

The Certificate Manager is authorised by the relying party to:

- submit an application under the RA process to hold a certificate on behalf of the relying party
- complete, sign, and lodge the necessary documentation that provide EOI of both the relying party and the Certificate Manager
- request additional certificates as required for use by other representatives of the relying party under the RA process
- undertake the obligations set out in Section 9.6.3.3.

1.3.4.3Policy Management Authority

VANguard is responsible for maintaining this CPS, and for the compliance audit for the CA that issues certificates in the MPKI hierarchy outlined in Section 1.4.

1.4 Certificate Usage

The appropriate certificate uses are defined in the CP and PDS for each certificate type and in the MOU and SLA entered into between VANguard and a relying party.

1.4.1 Appropriate Certificate Uses

The purpose of the OCA certificates and key pairs is to sign end-entity certificates and certificate status responses. This enables electronic transactions with, and on behalf of, relying parties and others, and allows a relying part to:

- authenticate electronically in online transactions
- digitally sign documents, transactions and communications
- confidentially communicate with a relying party.

A certificate is suitable for supporting the transmission of information from Unclassified up to and Sensitive DLMs, except Sensitive: Cabinet in accordance with the Australian Government Protective Security Policy (PSPF).

The use of certificates for transactions containing sensitive information (eg In Confidence or Highly Protected) may be restricted by the individual transacting parties.

1.4.2 Prohibited Certificate Uses

VANguard has specifically limited its liability in respect of certificates as specified in Section 9.8 of this CPS.

Prohibited certificate uses are defined in the CP, and in the PDS and SLA entered into between VANguard and the relying party.

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

The organisation administering this document is the VANguard Program.

1.5.2 Contact Person

Enquiries in relation to this CPS should be directed to VANguard.Customer@industry.gov.au

Refer to the applicable SLA for information regarding the VANguard MPKI functions including support contact details and support hours.

1.5.3 Person Determining CPS Suitability for the Policy

The VANguard Policy Approval Authority (PAA) is the final authority that determines the suitability and applicability of the Gatekeeper CPS.

The PAA is responsible for the governance of the PKI within VANguard. The VANguard General Manager is responsible for all policy approval and management functions.

1.5.4 CP Approval Procedures (Gatekeeper Accreditation)

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

1.6 Definitions and Acronyms

See the *VANguard Glossary* for acronyms and definitions used throughout this document.

2 Publication and repository responsibilities

2.1 Repositories

Symantec is responsible for the management and operation of repository functions related to the VANguard MPKI services. Symantec operates standard X.500 directory services in accordance with *ITU-T Recommendation X.500 (ISO/IEC 9594: Information Technology -- Open Systems Interconnection -- The Directory*.

2.2 Publication of Certification Information

Symantec is responsible for the VANguard RCA certificate, which contains only the VANguard RCA public key, and making it available to end entities on the VANguard Enrolment Page available on the Symantec website.

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

This CPS, the *Relying Party CP*, and the *Relying Party PDS* policy documents are available on the VANguard website. Other documentation may be available on request.

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance with Section 9.12. Updates to SLAs are published as required.

VANguard updates the certificate directory as soon as practicable whenever a new certificate is issued. Updates to the CRL occur at least once daily. Relying Party certificate information is published when it is made available.

2.4 Access Controls on Repositories

Read only access is provided to this CPS, and other approved documents such as the SLA, either on the VANguard website, or on request.

Access to the certificate directory and the CRL is not provided.

3 Identification and authentication

3.1 Naming

3.1.1 Types of Names

The VANguard MPKI assigns an X.500 Distinguished Name (DN) to each issued certificate based on the registration information.

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

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

The VANguard MPKI may refuse to assign a DN based on the registration information on reasonable grounds, for example where the DN is considered to:

- be obscene or offensive
- mislead or deceive (including where the pseudonym has already been issued to an individual)
- infringe the intellectual property (IP) rights of any person
- otherwise be contrary to law.

3.1.2 Need for Names to be Meaningful

DNs that are created based on authenticated EOI are assumed to be meaningful. Names must be unambiguous and unique and sufficiently detailed to enable identification of the relying party.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous and pseudonymous certificates are not supported.

3.1.4 Rules for Interpreting Various Name Forms

DNs must include each of the elements specified in the X.509-compliant certificate profile.

3.1.5 Uniqueness of Names

The Subject DN allocated by the VANguard MPKI will be unique to that certificate type. This is enforced by the software controls in the MPKI that ensure registration names are unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

Trademark rights, or other IP rights, may exist in the organisation's name, or other parts of the registration information or certificate information.

By applying for registration, the relying party:

- authorises the VANguard MPKI to use the relevant IP for the purpose of creating a DN, and for other purposes in relation to issuing keys and certificates to an organisation
- warrants that they are entitled to use that IP for which keys and certificates are issued and used, without infringing the rights of any other person
- agrees to indemnify the VANguard MPKI 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.

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

3.1.7 Name Claim Dispute Resolution

Disputes regarding assignment of DNs must be resolved under Section 9.13.

3.2 Initial Identity Validation

Formal identity verification means that all applicants undergo a face-to-face EOI check with an RA in accordance with Sections 3.2 through 3.4.

Initial verification establishes the identity of the individual key holders (in their capacity as representatives of organisations). For the issuance of digital certificates to individual key

holders, both the identity of the representative and the identity of the organisation are verified and identified within the digital certificate itself.

Additional steps are required to establish the authority of the Certificate Manager to hold and use a certificate on behalf of the organisation.

3.2.1 Method to Prove Possession of Private Key

The VANguard MPKI 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.

Where a key pair is generated by the VANguard MPKI on behalf of a relying party (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

Applications can be made for digital certificates by representatives of organisations (Certificate Managers and key holders). In terms of organisation identity, these applicants are authenticated in terms of the identity of the organisation as well as the binding of the person to the organisation.

The documents presented for establishing the organisation identity must:

- identify the organisation
- confirm that the named authoriser is a member of the organisation
- indicate that the authoriser has approved a Certificate Manager for the organisation.

VANguard will reject an application if the organisation's jurisdiction of incorporation, registration, or place of business is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business under Australian law

All data is transmitted and handled in accordance with the *VANguard Privacy Policy*.

For further details refer to the *VANguard Certificate Enrolment Procedure*.

3.2.2.1 Delegated RA Process

Not applicable.

3.2.3 Authentication of Individual Identity

Applications can be made for digital certificates by both individuals and representatives of organisations (including Certificate Managers and key holders). These applicants are authenticated in terms of the binding between the physical person and their documented identity. It is important for an RA to have sighted a document that bears a biometric signature or photograph.

Representatives of organisations are authenticated in terms of those bindings that apply to the Individual as well as the binding between the person and the organisation as described in Section 3.2.2.

The individual shall undergo identity verification by an accredited RA in accordance with the Gatekeeper EOI Policy found at the Digital Transformation Agency website.

For further details refer to the *VANguard Certificate Enrolment Procedure*.

3.2.4 Non-Verified Subscriber Information

The business unit within an organisation supplied in the certificate information is not verified.

RAs are not required to investigate or ascertain the authenticity of any document received by the RA as part of the registration process unless they are aware, or should reasonably be aware, that the document is not authentic.

For further details refer to the CP or PDS.

3.2.5 Validation of Authority

The individuals duly authorised in the roles of key holder and Certificate Manager should be validated prior to acting in their respective roles.

For further details refer to the CP or PDS.

3.2.5.1 Role of Authoriser

The RA shall verify the authorisation of a person identified by a relying party. Authorisation of the individual's association with the organisation must be evidenced by reference to:

- an authoritative public register; or
- appropriate legal, or regulatory documents issued by a government agency.

3.2.5.2 Role of Certificate Manager

Prior to issuance of a certificate containing an organisation identity, the intended Certificate Manager's binding to the organisation named in the certificate shall be established by a

formal letter of authorisation from an authoriser (sighted by the RA) that the individual is authorised to apply for a digital certificate and act in the role of Certificate Manager on behalf of the relying party.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

Not applicable.

VANguard does not permit rekey 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.

Relying parties applying for the issue of a new certificate after revocation must apply for a new certificate online. A new certificate can be applied for with the same DN. VANguard then approves the issuing of this new certificate.

3.4 Identification and Authentication for Revocation Request

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 in accordance with Section 4.9.2.

4 Certificate life-cycle operational requirements

The RA maintains an *RA Operations Manual* that details the operational practices of the RA in relation to its functions and obligations under this CPS. This is a confidential internal document that is not publicly available.

4.1 Certificate Application

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

4.1.1 Who Can Submit a Certificate Application?

A relying party can apply to the VANguard RA for a certificate. A relying party can only have one certificate with the same DN, 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 **Error! Reference source not found.** Initial Identity Validation.

4.1.2 Enrolment Process and Responsibilities

Under the RA process, the Certificate Manager accepts responsibility for the certificate through acceptance of an MOU and SLA with the VANguard MPKI.

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

Applicants are authenticated in accordance with Section 3.2.

Applicants must provide sufficient EOI information and be verified in accordance with Section 3.2 Initial Identity Validation.

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

4.2.2 Approval or Rejection of Certificate Applications

The VANguard MPKI is not obligated to issue certificates to any person despite receipt of an application. An application that has not successfully provided proof of identity shall be rejected by the RA. 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

RAs begin processing certificate applications within a reasonable time of receipt and endeavour to process applications with 48 hours of receipt.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Upon certificate issuance, the certificate is securely delivered to the relying party confirmed to have possession of the private key corresponding to the signed public key.

The OCA creates a certificate based on the information contained in the approved certificate application following successful authentication of the relying party in the installation process.

Once a certificate is downloaded by a relying party, the VANguard MPKI will have no continuing duty to monitor or investigate the continuing accuracy of the information in a certificate.

The OCA, 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 **Error! Reference source not found. Error! Reference source not found.**
- 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

VANguard will notify relying parties that they have created a certificate, and access to their certificates.

After the RA approves an enrolment request, they send an approval email using the email address provided in the certificate enrolment application. This notifies the relying party that the certificate has been issued and is available for acceptance. Instructions for downloading and accepting the certificate are provided in the email.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Downloading the certificate by a relying party constitutes acceptance.

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 OCA has signed the certificate. The email address used is that provided in the registration information. The status in the repository is then changed from pending to valid.

The applicant must notify the RA of any inaccuracy or defect in the information in a certificate promptly after receipt of the certificate, 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 MPKI shall have no continuing duty to monitor or investigate the accuracy of the information in a certificate, unless notified in accordance with the 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

Certificates will be published after issue in accordance with Section 2.3.

The MPKI 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

The MPKI does not automatically notify other entities of the issuance of the certificate.

RAs receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate is only permitted once the relying party has agreed to the MOU and SLA and accepted the certificate. The certificate shall be used lawfully in accordance with the SLA, the terms of the CP, and the PDS.

Relying parties shall protect their private keys from unauthorised use and shall discontinue use of the private key following expiration or revocation of the certificate.

For further information refer to the CP or PDS

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable SLA as a condition of relying on the certificate.

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, relying parties will independently assess:

- the appropriateness of the use of a certificate for any given purpose and determine that the certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by the CP. VANguard is not responsible for assessing the appropriate use of a certificate
- that the certificate is being used in accordance with the *KeyUsage* field extensions included in the certificate (eg if a Digital Signature is not enabled then the certificate may not be relied upon for validating a signature), and as per Section 6.1.7
- the status of the certificate and the OCA that issued the certificate in accordance with Section 4.9.6. If any of the certificates have been revoked, the relying party is solely responsible to investigate whether reliance on a digital signature prior to revocation is reasonable. Any such reliance is made solely at the risk of the relying party.

Assuming that the use of the certificate is appropriate, relying parties shall use the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on certificates in connection with each such operation. Such operations include verifying the digital signatures on all certificates.

For further information refer to the CP or PDS.

4.6 Certificate Renewal

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

Technically, certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. This is not supported for the MPKI.

See Section 4.7 Certificate Re-Key.

4.7 Certificate Re-Key

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

Prior to the expiration of an existing certificate, it will be necessary for the relying party to obtain a new certificate to maintain continuity of certificate usage. The MPKI requires that the relying party generate a new key pair to replace the expiring key pair.

VANguard will notify the certificate holder via the email address on the certificate prior to the expiry of the certificate. The email shall contain instructions on how to renew the digital certificate.

4.7.1 Circumstances for Certificate Re-Key

Not applicable.

Expiration of a certificate does not affect the validity of any underlying contractual obligations created under this CPS or the CP.

Renewal of a revoked certificate is not permitted after revocation regardless of the reason for revocation. Following revocation, a relying party may request a replacement certificate as described in Section 3.3.2.

4.7.2 Who May Request Certification of a New Public Key

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

4.7.3 Processing Certificate Re-Key or Replacement Requests

Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of the issuance of a certificate to the relying party is in accordance with Section 4.3.2. **Error! Reference source not found.**.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section **Error! Reference source not found. Error! Reference source not found.**.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section **Error! Reference source not found.** Publication of the Certificate by the CA.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

Not applicable. VANguard does not support certificate modification.

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the public key).

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 Circumstances for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section **Error! Reference source not found. Error! Reference source not found.**.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section **Error! Reference source not found. Error! Reference source not found.**.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

On revocation of a certificate:

- the certificate's operational period expires
- the underlying contractual obligations between the organisation and other VANguard MPKI entities are unaffected
- the relying party must continue to safeguard their private keys unless they destroy their private keys
- the relying party must cease using the certificate for any purpose whatsoever
- the VANguard MPKI must promptly notify the relying party that its certificate has been revoked
- the VANguard MPKI must update the CRL.

4.9.2 Circumstances for Revocation

The VANguard MPKI shall revoke a certificate on request of a person specified in Section 4.9.3, or whether or not it has received a request to do so, or where it becomes aware of (or reasonably suspects) the following:

- upon failure of the relying party to meet its material obligations under this CPS, CP, or any other agreement, regulation, or law applicable that may be in force
- if knowledge or reasonable suspicion of compromise is obtained
- if it is determined that the certificate was not properly issued in accordance with this CPS or CP
- if the relying party has ceased to belong to a specified/agreed Community of Interest
- on request by a person specified in Section 3.2.5 **Error! Reference source not found.**, or where the key holder ceases to be an employee or agent of the organisation
- 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 or certificate information occurs
- the key holder's/certificate's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability
- the applicable relying party has not complied with an obligation under this CPS, the CP, or the SLA
- another person's information has been or may be materially threatened or compromised unless the certificate is revoked.

The MPKI is not required to investigate any of the circumstances for revocation, but in cases where the circumstances are investigated, they must use reasonable efforts to notify the relevant relying party beforehand of that intention.

Certificates should be revoked where any one of the following circumstances arises:

- a private key is compromised
- media holding a private key is compromised or lost
- the key holder (in this instance is the device/application) ceases to exist
- there has been improper or faulty issuance of the device keys and certificates
- the certificate information becomes inaccurate
- a change in the registration information occurs
- the VANguard MPKI ceases to operate
- the organisation ceases to exist
- the VANguard MPKI receives a revocation request from an authoriser or a Certificate Manager.

4.9.3 Who Can Request Revocation

A relying party, or an authorised representative, can request the RA to revoke the certificate(s) at any time.

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 relying party.

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).

Relying parties can request revocation of their certificates. However, 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.

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.

4.9.4 Procedure for Revocation Request

A revocation request may be submitted in person, or sent to the VANguard RA by any of the methods identified in Section 9.11 **Error! Reference source not found.**.

A revocation request, which is made in person, must be made to the RA at the address set out on the VANguard website.

A request is authenticated in accordance with Section 3.4.

A request (including an order or direction) will be processed only if the RA is satisfied that the entity is lawfully empowered to request revocation of the certificate.

Upon revocation of a certificate the RA must promptly notify the relying party that its certificate has been revoked and update the CRL. Upon revocation of a certificate the certificate's operational period ends/expires.

VANguard will:

- issue a notice to the relying party confirming the revocation of the keys and certificate and the date and time that the certificate is revoked. The list of revoked certificates is made accessible to potential relying parties through either LDAP or OCSP

- 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.

4.9.5 Revocation Request Grace Period

The request for certificate revocation shall be processed expeditiously. The request for certificate revocation must be investigated and accessed via mechanisms that balance the need to quickly revoke the certificate for reasons of compromise against the need to prevent unauthorised or unwarranted requests.

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

4.9.6 Time within Which CA Must Process the Revocation Request

Revocation requests are processed immediately upon receipt from the RA, and are processed within 24 hours.

4.9.7 Revocation Checking Requirement for Relying Parties

See Section 9.6.4 Relying Party Representations and Warranties.

4.9.8 CRL Issuance Frequency (If Applicable)

The OCA will update the CRL for relying party certificates at least daily. CRLs for the OCA shall be issued every 12 hours (noon and midnight), but at least quarterly, and also whenever a certificate is revoked. They are valid for 24 hours.

CRLs can also be issued on an emergency basis.

4.9.9 Maximum Latency for CRLs

CRLs are posted to the repository automatically within minutes of generation, but at least one day.

4.9.10 On-Line Revocation/Status Checking Availability

Online revocation and other certificate status information are available via a web-based repository and, where offered, OCSP. A web-based repository permits relying parties to make online inquiries regarding revocation and other certificate status information.

The appropriate URL of the OCSP responder (if any) to determine the validity of a certificate in real time can be determined from information appearing in the certificate.

4.9.11 On-line Revocation Checking Requirements

Prior to placing reliance upon a certificate, a relying party must check the status of the certificate in accordance with Section 9.6.4.1. Otherwise there is no stipulation.

4.9.12 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.13 Special Requirements Regarding Key Compromise

VANguard shall use commercially reasonable efforts to notify potential relying parties if they discover, or have reason to believe, that there has been compromise of the private key of the OCA or RCA.

4.9.14 Circumstances for Suspension

Certificate suspension is not currently supported for certificates.

4.9.15 Who Can Request Suspension

Not applicable.

4.9.16 Procedure for Suspension Request

Not applicable.

4.9.17 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

In the revocation of certificates, VANguard shall provide access to digital certificate status information via an approved X.509 compliant protocol (eg DAP, LDAP or OCSP). VANguard is not confined to using a single protocol for the distribution of certificate information, but will ensure that information in directories is synchronised.

4.10.1 Operational Characteristics

A relying party will be able to ascertain the status of a certificate by consulting the certificate LDAP directory and the CRL at a URL specified in the CP.

4.10.2 Service Availability

Certificate status services shall be available 24 X 7 excepting scheduled interruption.

Refer to the applicable SLA.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

A relying party may end a subscription for a certificate by:

- allowing the certificate to expire without renewing or re-keying that certificate
- requesting revocation of the certificate before certificate expiration without replacing the certificate.

Otherwise there is no stipulation.

4.12 Key Escrow and Recovery

VANguard does not support key escrow.

Relying parties are responsible for their own arrangements regarding key escrow.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, management and operational controls

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 MPKI are undertaken.

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

VANguard conforms to the standards and guidelines stipulated by the Australian Signals Directorate (ASD) *Information Security Manual* (ISM) where applicable.

5.1 Physical Controls

Symantec implements physical controls and security to ensure that they are able to provide their services in a secure, reliable and trusted manner.

Symantec's Gatekeeper accredited Protective Security Plan (PSP) details the physical controls in place for the VANguard MPKI, 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.

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

All Digicert Gateway CA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of sensitive information and systems.

Such requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or gate that provides mandatory access control for

individuals and requires a positive response (eg door or gate unlocks or opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorised access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside wall of the building.

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 PROTECTED information.

5.1.2 Physical Access

Access to each tier of physical security shall be auditable and controlled so that each tier can be accessed only by authorised personnel. Sensitive materials, including CA cryptographic hardware and associated key material when not in use, are securely stored within storage containers with security strength commensurate with the sensitivity of the materials being stored. Access shall be auditable and controlled to ensure access by only authorised and trusted personnel in accordance with Section 5.2.2.

Digicert 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.

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

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

The secure facilities of CAs shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Each site has backup power supplies including diesel generators as a fail-safe power supply. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity. The generators provide power on a priority basis to key services and areas.

5.1.4 Water Exposures

The secure facilities of CAs shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water.

5.1.5 Fire Prevention and Protection

The secure facilities of CAs shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage

Digicert shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorised use of, access to, or disclosure of such media.

Media containing information on the VANguard MPKI 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

Digicert shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorised use of, access to, or disclosure of waste containing Confidential/Private Information.

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

5.1.8 Off-Site Backup

Digicert shall maintain back-ups of critical system data or any other sensitive information, including audit data, in a secure off-site facility.

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

5.2 Procedural Controls

5.2.1 Trusted Roles

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be ‘Trusted Persons’ serving in a ‘Trusted Position.’ Persons seeking to become Trusted Persons by obtaining a Trusted Position require background screening.

Trusted Persons include all employees, contractors, and consultants that have access to, or control authentication or cryptographic operations, that may materially affect the processing, issuance, or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of relying party information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel
- system administration personnel
- designated engineering personnel
- executives that are designated to manage infrastructural trustworthiness.

Digicert staff involved in VANguard CA operations are identified as Positions of Trust in the Digicert Trusted Employee Policy. This policy describes the procedures that are implemented to ensure that appropriate screening is performed. The screening varies with the duties staff must perform.

5.2.2 Number of Persons Required Per Task

Digicert shall establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold ‘Secret Shares’ and vice versa.

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

Digicert shall confirm the identity and authorisation of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities
- given electronic credentials to access and perform specific functions on systems.

Authentication of identity shall include the personal (physical) presence of such personnel in front of Trusted Persons performing HR or security functions, and a check of well-recognised forms of identification, such as passports and driver’s licenses. Identity shall be further confirmed through background checking procedures specified in this CP.

The Digicert 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

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 of the repository
- the handling of relying party information or requests
- the generation, issuing or destruction of a CA certificate
- the loading of a CA to a Production environment.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Digicert shall require that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

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

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

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 Digicert Trusted Employee Policy.

VANguard staff are cleared to Baseline as per the Department's Employment Procedures. Some staff are cleared to NV1 dependent on their role.

5.3.2 Background Check Procedures

Background checks in accordance with Baseline and NV1 standard are conducted through the Australian Government Security Vetting Agency (AGSVA).

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person.

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

5.3.3 Training Requirements

VANguard shall provide their staff with the requisite training needed to perform their job responsibilities relating to CA or RA operations competently and satisfactorily. They shall also periodically review their training programs, and their training shall address the elements relevant to functions performed by their personnel. Such training programs shall address the elements relevant to the particular environment of the staff being trained.

5.3.4 Retraining Frequency and Requirements

VANguard shall provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

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

VANguard shall establish, maintain, and enforce employment policies for the discipline of personnel following unauthorised actions. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorised actions.

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

5.3.7 Independent Contractor Requirements

VANguard may permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly-defined outsourcing relationships and only under the following conditions:

- the entity using the independent contractors or consultants as Trusted Persons does not have suitable employees available to fill the roles of Trusted Persons

- the contractors or consultants are trusted by the entity to the same extent as if they were employees.

Otherwise, independent contractors and consultants shall have access to the VANguard secure system only to the extent they are escorted and directly supervised by Trusted Persons.

Section **Error! Reference source not found.** Personnel Controls applies to any staff member within VANguard MPKI operations.

5.3.8 Documentation Supplied to Personnel

VANguard shall provide their personnel (including Trusted Persons) with the requisite training and access to other documentation needed to perform their job responsibilities competently and satisfactorily.

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

5.4 Audit Logging Procedures

The CAs are required to log particular information. The SSP details the audit logging procedures required to maintain a secure environment.

5.4.1 Types of Events Recorded

All logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event. The types of auditable events logged by the CA include:

- operational events (including but not limited to:
    - the generation of a CA's own keys and the keys of subordinate CAs
    - start-up and shutdown of systems and applications
    - changes to CA details or keys, cryptographic module lifecycle management-related events (eg receipt, use, de-installation, and retirement)
    - possession of activation data for CA private key operations, physical access logs
    - system configuration changes and maintenance
    - records of the destruction of media containing key material, activation data, or personal relying party information
- certificate lifecycle events (including, but not limited to, initial issuance, revocation, suspension)

- trusted employee events (including but not limited to logon and logoff attempts, attempts to create, remove, set passwords or change the system privileges of the privileged users, personnel changes)
- discrepancy and compromise reports (including but not limited to unauthorised system and network logon attempts)
- changes to certificate creation policies, eg validity period.

The following events are recorded in audit log files:

- system start-up and shutdown
- CA 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.

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 relying parties.

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed in response to alerts based on irregularities and incidents within their CA/RA systems. Audit logs are continuously processed by centralised logging. Audit log reviews shall include a verification that the log has not been tampered with and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews shall be documented.

VANguard will review its audit logs in response to alerts based on irregularities and incidents within the VANguard CA and RA system. VANguard 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

Audit logs will be retained for at least 15 days after processing and then archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created every 15 minutes and full backups are performed are overnight.

5.4.6 Audit Collection System (Internal vs. External)

The audit collection system is maintained internally.

5.4.7 5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organisation, device, or application that caused the event.

There will therefore 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

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments (LSVAs) are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity's annual Compliance Audit.

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

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

5.5 Records Archival

In terms of the archival of records, VANguard complies with the *Archives Act 1983 (Cth).*

Notwithstanding the sub-sections below, archival of certificate information may be subject to jurisdictional legislation and other legal constraints which may override the conditions described.

The Digicert PSP includes general records archival and records retention policies.

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.

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

Digicert archives:

- all audit data collected in terms of Section 5.4
- certificate application information
- documentation supporting certificate applications
- certificate lifecycle information, eg revocation, rekey and renewal application information.

Most of the information collected by the VANguard RA is archived. See Section **Error! Reference source not found. Error! Reference source not found.**.

5.5.2 Retention Period for Archive

Audit trail information shall be kept for a minimum period of seven (7) years from the date of generation, unless the organisation specifically requires a longer period.

Records are retained in relation to certificates (including personal information) for seven years (7) after the date the certificate expires or is revoked.

For further information refer to the *VANguard Privacy Policy*.

5.5.3 Protection of Archive

The archive of records shall be accessible by only authorised Trusted Persons. The archive is protected against unauthorised viewing, modification, deletion, or other tampering by storage within a Trustworthy System. Archive media shall be protected either by physical security or a combination of physical security and cryptographic protection. It shall also be protected from environmental factors such as temperature, humidity, and magnetism.

The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in Section 5.5.2.

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

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

Copies of paper-based records shall be maintained in a secure facility.

5.5.5 Requirements for Time-Stamping of Records

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

The following records are time stamped:

- certificates
- CRLs and other revocation databases
- customer service messages.

5.5.6 Archive Collection System (Internal vs. External)

The archive collection system is maintained internally.

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

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorised Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

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

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

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

The RAs will ensure that key changeover causes minimal disruption to relying parties, and provide reasonable notice of any planned changeover.

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

Digicert 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 MPKI
- compromise of the VANguard CA private keys which relying parties rely on to establish trust in certificates.

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

5.7.1 Incident and Compromise Handling Procedures

Backups of CA information including certificate application data, audit data, and database records for all certificates issued, shall be kept in off-site storage and made available in the event of a compromise or disaster. The Digicert DR&BCP covers all reasonably foreseeable types of disasters and compromises affecting the services under this CPS including:

- loss or corruption (including suspected corruption) of computing resources, software, and/or data of the Digicert CA or another PKI Service Provider
- compromise of the Digicert CA's private keys which relying parties rely on to establish trust in certificates.

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

VANguard at its discretion may report security incidents to relying parties if the assurance of the VANguard MPKI is compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

Following corruption of computing resources, software, and/or data, a report of the incident and a response to the event, shall be promptly made by the affected CA or RA in accordance with Symantec's documented incident and compromise reporting and handling procedures in the applicable CPS and security policies.

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

5.7.3 Entity Private Key Compromise Procedures

If a private key of a CA is compromised, the VANguard RCA will revoke the CA's certificate, (including as a result of compromise), and report the revocation in the CRL and in the repository. See Section **Error! Reference source not found.** Incident and Compromise Handling Procedures.

5.7.4 Business Continuity Capabilities After a Disaster

Digicert operating secure facilities develop, maintain, annually test and, when necessary, implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans address the restoration of information systems services and key business functions. Disaster recovery sites have the equivalent physical security protections specified by this CP.

Digicert has the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions: certificate issuance, certificate revocation and publication of revocation information.

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

5.8 CA or RA Termination

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
- for reliance on Digital Signatures or certificates.

VANguard will give as much notice as possible of the relevant circumstances, and the actions it proposes to take to:

- all relying parties
- the relying parties of which VANguard is aware.

If a PKI Service Provider (including the Digicert CA itself) unexpectedly ceases providing services the CA must immediately give notice to the affected parties to provide them the opportunity to address any business impacting issues.

In the event that the OCA ceases operations, all certificates issued by the OCA shall be revoked prior to the date that the OCA ceases operations. The obligations for termination under this section are in addition to any obligations the Digicert CA or any other entity has under the requirements set forth in Section 5.7 Compromise and Disaster Recovery.

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

Where VANguard intends to terminate its own services, it will attempt to give at least three (3) months' notice to the affected parties.

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

The obligations under this section are in addition to any obligations under the requirements of Section **Error! Reference source not found.** Representations and Warranties.

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

6 Technical security controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

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.

Keys for the CAs are generated by the RCA; keys for relying parties are generated by the OCA.

CA keys are generated in a key generation ceremony. All key generation ceremonies are conducted in accordance with confidential security policies.

A relying party's key pair(s) are generated and stored by the application that generates those keys (eg a browser) during the application process. Key pair generation is performed in accordance with the *Key Management Plan* (KMP), and the *VANguard Certificate Enrolment Procedure*.

6.1.2 Private Key Delivery to Subscriber

As the relying party's private keys are generated and stored by the relying party's application (eg a browser), there is no need to see or deliver any private keys to relying parties. The VANguard MPKI does not deliver its CA private keys to any entity.

Refer to the CP and PDS for relying party private key delivery information.

6.1.3 Public Key Delivery to Certificate issuer

A relying party's public key is forwarded to the OCA as part of the key generation process. When a public key is transferred to the CA to be certified, it shall be delivered through a mechanism ensuring that the public key has not been altered during transit and that the relying party possesses the private key corresponding to the transferred public key such as a PKCS#10 message or other cryptographically equivalent method.

Upon the relying party's acceptance of the certificate, the CA shall publish a copy of the certificate in the certificate directory and in other appropriate locations, as determined by the CA. See Section **Error! Reference source not found. Error! Reference source not found.**.

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

The OCA's application process checks the key size of keys and ensures that all keys generated by the applicant are 2048 bits or longer.

Key pairs are generated by the relying party using algorithms embedded in the application/hardware used to generate the keys. These algorithms should be of the strength and type specified on the EPL.

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

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 EPL.

6.1.7 Key Usage Purposes (as per x509v3 field)

Key usage is defined in accordance with RFC 5280 for X.509 version 3 certificate. Single-use certificates shall be issued as follows:

- encryption certificate with key usage set to *KeyEncipherment* and *DataEncipherment*.
- signing certificate with key usage set to *DigitalSignature*.

Additional information on key usage is provided in the certificate profile in Section 7.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

Relying parties should instigate their own policies to ensure the integrity, and security of their private keys. Private keys shall be protected using a trustworthy system and relying parties shall take necessary precautions to prevent the loss, disclosure, modification or unauthorised use of such private keys.

The VANguard MPKI uses mechanisms detailed in the KMP to protect its private keys from loss, disclosure, modification or unauthorised use. Private keys are subject to multi-person

control over activation of or access to the hardware cryptographic device containing the private key in accordance with Sections 5.2.2 and 5.2.3.

6.2.1 Cryptographic Module Standards and Controls

Private keys within the VANguard MPKI are protected using a trustworthy system.

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

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

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

Not applicable. VANguard does not use multi-person controls.

6.2.3 Private Key Escrow

The VANguard MPKI does not escrow the OCA private keys.

6.2.4 Private Key Backup

VANguard backs up the OCA private keys to enable recovery from disasters and equipment malfunction in accordance with confidential security policies. Backups are made by copying the OCA private keys and entering them onto backup cryptographic modules in accordance with Section 6.2.6 and 6.2.7.

Private keys that are backed up are protected from unauthorised modification or disclosure through physical or cryptographic means. Backups are protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules onsite and at another secure off-site facility.

Relying parties may make their own arrangement for backup of their private keys used for decryption. Backup of keys with key usage set to *Digital Signature* is discouraged.

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

Private key backup is not provided for relying parties.

6.2.5 Private Key Archival

The VANguard MPKI keeps a copy of all private keys it has used. Upon expiration of a certificate, the key pair associated with the certificate is securely retained for a period of at least five (5) years using hardware cryptographic modules that meet the requirements of the CP. These key pairs shall not be used for any signing events after the expiration date of the corresponding certificate, unless the certificate has been renewed in terms of the CP.

A private key archive is not provided for relying parties. Organisations may make their own arrangement for archival of historical private keys used for encryption. Upon expiration the private keys used for signing are no longer used and archiving is not required.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

Entry of a private key into a cryptographic module shall use mechanisms to prevent loss, theft, modification, unauthorised disclosure, or unauthorised use of such private key.

The generation of private keys on one hardware cryptographic module and transferring them into another shall be performed securely to the extent necessary to prevent loss, theft, modification, unauthorised disclosure, or unauthorised use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens in accordance with confidential security policies. Private keys shall be encrypted during such transfer.

The relying party should ensure that their private keys are entered into a cryptographic module (eg software key store) in an appropriate manner to prevent loss, theft, modification, unauthorised disclosure, or unauthorised use of such private keys.

6.2.7 Private Key Storage on Cryptographic Module

Private keys held on hardware cryptographic modules are stored in encrypted form. A trustworthy hardware device operating within a processing centre is used to create, protect, and store the VANguard MPKI private keys.

6.2.8 Method of Activating Private Key

Activation of the RCA private key requires multi-person control in accordance with Section 6.2.2.

For private key protection, VANguard uses a cryptographic module that requires them to:

- present the cryptographic module along with a password in accordance with Section 6.4.1 to authenticate the RA before the activation of the private key; and

- take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the RA's authorisation.

It is strongly recommended that the key holder (including Certificate Managers serving in the role of delegated RA) restrict access to the private key by use of activation data, so that before an operation requiring the private key may be commenced the activation data known only to the key holder must be entered. The use of two factor authentication mechanisms (eg token and passphrase, biometric and token, or biometric and passphrase) is encouraged. Relying parties have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys.

6.2.9 Method of Deactivating Private Key

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

The relying party should ensure that their private keys are deactivated after usage in an appropriate manner to prevent unauthorised use of such private keys.

6.2.10 Method of Destroying Private Key

Private keys are destroyed in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key in accordance with the ISM. Such a process shall be witnessed in accordance with VANguard confidential security policies.

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

6.2.11 Cryptographic Module Rating

Cryptographic modules used in the VANguard MPKI use software listed on the ASD EPL. See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The VANguard MPKI archives the public keys of its CAs. The archived public keys are located in the repository and are stored for seven (7) years in accordance with the *Australian National Archives Policy.*

There is no stipulation for relying parties.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The OCA shall not issue certificates with operational periods that extend beyond the usage period of the key pair. Therefore, the OCA key pair usage period is necessarily shorter than the operational period of the OCA certificate and the OCA shall be recertified two years prior to the expiry of the certificate (specifically, the length of the operational period of the end entity certificates that the OCA issues).

Upon the end of the operational period for an OCA key pair, the OCA will cease all use of the key pair, except to the extent a CA needs to sign revocation information until the end of the operational period of the last certificate it has issued.

The operational period for relying party key pairs is the same as the operational period for their certificates, except that keys may continue to be used after the operational period for data decryption and signature verification. The operational period of a certificate ends upon either its expiration or revocation. Relying parties shall cease all use of their authentication (signing) private key at the end of the operational period.

The RCA has a minimum 4096-bit RSA key length and 24 year certificate validity period.

The usage period for the OCA public and private keys is 23 years.

The usage period for the relying party public and private keys is four (4) years.

6.4 Activation Data

Activation data refers to data other than the keys that are required to operate cryptographic modules (eg password and pins).

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

6.4.1 Activation Data Generation and Installation

Not applicable.

6.4.2 Activation Data Protection

Not applicable.

6.5 Computer Security Controls

The *VANguard Security Risk Management Plan* (SRMP) covers security of VANguard operations and systems used to provide computer security.

6.5.1 Specific Computer Security Technical Requirements

The VANguard production network is logically separated from other components to prevent network access except through defined and authorised application processes.

Direct access to the VANguard system and repositories shall be limited to trusted persons having a valid business reason for such access.

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

6.5.2 Computer Security Rating

VANguard meets the requirements of the Australian Government's information security standards.

6.6 Life Cycle Technical Controls

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

6.6.1 System Development Controls

VANguard shall adopt system development controls as specified within the *Protective Security Policy Framework (PSPF)*.

Digicert 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

See Section 6.6.1.

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

The CAs are operated in an offline (non-networked) mode. Under no circumstances are the servers networked in any fashion.

CA functions are performed using networks secured in accordance with confidential security policies to prevent unauthorised access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

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.

Network security controls are specified in the SSP and the SRMP which identify and address all high or significant life cycle security threats.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

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

See Section **Error! Reference source not found. Error! Reference source not found.**.

7 Certificate, CRL and OCSP profiles

7.1 7.1 Certificate Profile

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

7.1.1 End Entity Certificates

Refer to the VANguard CPs for detailed certificate profiles.

7.1.2 Version Number(s)

The VANguard MPKI supports and uses X.509 Version 3 certificates.

7.1.3 Certificate Extensions

The VANguard MPKI supports and uses X.509 Version 3 certificate extensions.

7.1.4 Algorithm Object Identifiers

The VANguard MPKI uses only those cryptographic algorithms approved by ASD.

OIDs are not allocated to algorithms in the VANguard MPKI.

7.1.5 Name Forms

Certificates issued under this CPS and CPs must contain the full DN of the CA issuing the certificate in the ‘Issuer’ field, and the organisation in the ‘Subject’ field in accordance with the certificate profiles, Section 7.1.1.

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

7.1.6 Name Constraints

Anonymous or pseudonymous names are not supported.

7.1.7 Certificate Policy Object Identifier

VANguard supports the use of the certificate policy OIDs as is indicated in the certificate profile.

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.

See the CP or PDS.

7.1.8 7.1.8 Usage of Policy Constraints Extension

Not applicable.

7.1.9 Policy Qualifiers Syntax and Semantics

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

See the CP or PDS.

7.1.10 Processing Semantics for the Critical Certificate Policies Extension

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

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

The 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'.

7.2.1 Version Number(s)

The VANguard MPKI supports and uses X.509 Version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

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

7.3.1 Version Number(s)

Not applicable.

7.3.2 OCSP Extensions

Not applicable.

8 Compliance audit and other assessments

8.1 Frequency or Circumstances of Assessment

Digicert is required to conduct periodic audits of its operations. Additionally, in accordance with Gatekeeper requirements, the Digicert MPKI must undergo an annual compliance audit by a member of the Audit Panel listed on the Gatekeeper website.

VANguard processes are covered by this audit. VANguard has a separate listing with Gatekeeper to operate as a Validation Authority.

The VANguard SM is responsible for ensuring the security of VANguard operations and is appointed by the VANguard GM. The VANguard SM may conduct audits if required by the VANguard GM.

VANguard will conduct regular Infosec - Registered Assessor Program (IRAP) assessments against the requirements of the ISM.

8.2 Identity/Qualifications of Assessor

Gatekeeper auditors are approved by the competent authority on the basis of expertise in relation to digital signature technology, information technology security procedures or any other relevant areas of expertise required of an auditor to enable evaluation to be carried out properly and expertly against the accreditation criteria.

8.3 Assessor's Relationship to Assessed Entity

Gatekeeper auditors will be independent of the audited entity.

IRAP auditors will be independent of the audited entity.

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

8.4 Topics Covered by Assessment

The purpose of a Gatekeeper audit is to ensure that a VANguard MPKI:

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

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

8.5 Actions Taken as a Result of Deficiency

Actions recommended by the auditor arising from any deficiency revealed by a Gatekeeper audit will be discussed by the audited entity and authorised representatives. If necessary, the competent authority may direct the audited entity to take certain remedial action. Failure to adequately address deficiencies identified in an audit may result in withdrawal of the entity's Gatekeeper accreditation.

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

8.6 Communication of Results

VANguard may release information to relying parties if the information will affect the assurance of the VANguard MPKI.

The date on which the Digicert Gatekeeper CA was last audited will be published on the Digicert Gatekeeper website, and may also be published by the Digital Transformation Agency (DTA).

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

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

9 Other business and legal matters

This CPS serves as notice of the rules governing the respective rights and obligations of the MPKI entities among themselves.

Refer to the CP and PDS.

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

Not applicable.

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

Not applicable.

9.1.5 Refund Policy

Not applicable.

9.2 Financial Responsibility

Refer to the CP and PDS.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

VANguard does not provide any insurance and/or extended warranty coverage for end-entity certificates issued to its relying parties.

9.3 Confidentiality of Business Information

Refer to the CP and PDS.

9.3.1 Scope of Confidential Information

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

Refer to the MOU and SLA between VANguard and the relying party.

9.3.2 Information Not Within the Scope of Confidential Information

Data supplied by relying parties and placed within the certificate become public by its nature and therefore shall not be considered confidential information.

Certificates, certificate revocation and other status information, repositories of the VANguard MPKI, and information contained within them are not considered confidential/private information. This section is subject to applicable privacy laws.

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

9.3.3 Responsibility to Protect Confidential Information

VANguard participants receiving confidential information shall secure it from compromise and disclosure to third parties.

Refer to the SLA.

9.4 Privacy of Personal Information

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.

Section **Error! Reference source not found. Error! Reference source not found.** does not apply to personal information.

9.4.1 Privacy Plan

Registration information may contain personal information about key holders. The 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.

VANguard complies with their obligations under the *Privacy Act 1988*, including (where applicable) the Australian Privacy Principles (APPs) as established by the *Privacy Amendment Bill 2012*.

VANguard must also comply with:

- any privacy law applicable to service providers to that agency; and
- any other privacy obligations imposed by or in relation to that agency.

The subject of any personal information held by VANguard shall on request be provided with that information in accordance with the personal information access protocol, and the privacy obligations applicable under this CPS, and if there is any inconsistency between the two, in accordance with those privacy obligations.

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.

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

Personal information collected as part of the registration process transaction that is not contained within the certificate or the CRL 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

Personal information contained within the certificate is not deemed private. Relying parties agree to the publication, through the certificate directory and CRL, of any personal information which forms part of the certificate information.

Revocation of a certificate published in the CRL in accordance with this CPS is also not deemed private.

9.4.4 Responsibility to Protect Private Information

The registration information may contain personal information about key holders.

The 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.

9.4.5 Notice and Consent to Use Private Information

Subject to any applicable law or legal restriction, personal information held by VANguard about a relying party may be disclosed to a third party where the relying party has authorised the disclosure in writing.

Users provide their consent via the VANguard Business Identity Provision Point (BIPP) website to which agencies can send their business users to be authenticated.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

All intellectual property rights in any CPS, CP or PDS, or other document published by the VANguard MPKI, 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: Public Draft for Comment, v0.30, American Bar Association 2001.

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.

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

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 this CPS, the CP, PDS, or other approved documents, will not infringe the IP rights of a third party.

9.6 Representations and Warranties

This section sets out important obligations and responsibilities of VANguard operating under this CPS and CP.

Relying parties agree not to monitor, interfere with, or reverse engineer the technical implementation of the services provided by VANguard except as explicitly permitted upon prior written approval from VANguard.

9.6.1 CA Representations and Warranties

The issuing CAs must meet all the obligations set out in this section.

The CA, issuing a certificate to the relying party, will ensure that:

- the RA has confirmed that verification has been successfully completed in accordance with Sections 3.2 through 3.4
- the RA attests to have accurately transcribed the certificate information provided by the authoriser or Certificate Manager into the certificate
- all material information contained in the certificate is accurate
- the certificate contains all the elements required by the certificate profile.

The OCA neither generates nor holds the private keys of relying parties. The OCA cannot ascertain or enforce any particular private key protection requirements of any organisation or relying party as recommended in Section 6.

The OCA will:

- ensure the availability of a certificate directory and CRL in accordance with Section 4.10
- promptly revoke a certificate if requested by the relying party or as otherwise required in accordance with Section 4.9
- ensure that the date and time when a certificate is issued or revoked can be determined precisely.

The CA 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.

The RCA for the purposes of this CPS is the VANguard RCA.

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 the OCA issued under the VANguard MPKI hierarchy
- properly conduct the verification process described in Section **Error! Reference source not found.** Initial Identity Validation
- ensure the accuracy and completeness of any part of the certificate information which is generated or compiled by the 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 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 CP or PDS, and other approved documents.

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

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

The VANguard MPKI will manage their keys in accordance with Section **Error! Reference source not found. Error! Reference source not found.**.

The VANguard MPKI cannot ascertain or enforce any particular private key protection requirements of any organisation or relying party.

The VANguard MPKI will:

- ensure the availability of a certificate directory and CRL
- promptly revoke a certificate if required.

9.6.2 RA Representations and Warranties

The RA must:

- properly conduct the verification process in accordance with Sections 3.2 through 3.4
- ensure the accuracy and completeness of any part of the certificate information which is generated or compiled by the 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 organisation, 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 this CPS (in particular, Sections 9.3 and 9.4) and the approved documents.

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

9.6.3 Subscriber Representations and Warranties

The relying party representations and warranties pertain to all relying parties.

Where an organisation accepts keys and certificates issued under this CPS or CP, that entity is deemed to be bound by the provisions applicable to:

- the applicant – when it submits an application for a certificate
- the key holder – when it accepts the SLA itself or on behalf of the organisation.

Each applicant must securely generate his, her, or its own private key(s), using a trustworthy system, and take necessary precautions to prevent their compromise, loss, disclosure, modification, or unauthorised use. Applicants must comply with Section 6 of this CP.

Each certificate applicant acknowledges that they, and not VANguard, are exclusively responsible for protecting their private key(s) from compromise, loss, disclosure, modification or unauthorised use.

The relying party must notify VANguard 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.

A relying party 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 is deemed not valid.

Upon revocation of a certificate the certificate's operational period ends/expires and the relying party must:

- cease using the certificate for any purpose whatsoever
- continue to safeguard their private keys unless they destroy their private keys.

Upon revocation of a certificate the underlying contractual obligations between the relying party and VANguard are unaffected. See the PDS and the MOU between VANguard and the relying party.

9.6.3.1 Subscriber and/or Key Holder Obligations

The key holder refers to the individual named within the certificate. The key holder must:

- not delegate his or her responsibilities for the generation, use, retention, or proper destruction of his or her private keys with the exception of storage of keys for archival purposes and destruction of their private keys to a person authorised to perform that act on behalf of the organisation
- ensure that their private keys are not compromised
- immediately notify VANguard if they become aware that their private key has been compromised, or there is a substantial risk of compromise
- ensure that all information provided to the RA in relation to issue and use of their key pairs and certificates is to the best of their knowledge, true and complete
- immediately notify VANguard if there is any other change to their registration information, or any other information provided to the Digicert CA or the RA in relation to issue and use of their keys and certificates

- use keys and certificates only for the purposes for which they were issued and within the usage and reliance limitations, as specified in this CPS, the certificate profile and the certificate
- check the details set out in a certificate on receipt, and promptly notify VANguard if faulty or improper registration or certificate issuance has occurred
- if requested by the RA, provide complete and accurate information in relation to their registration information or anything else relating to issue or use of their keys and certificates
- use keys and certificates only for purposes for which they have the actual authority of the organisation
- they cease to be an employee or agent of their organisation
- they cease to be authorised to hold keys and certificates on behalf of their organisation.

9.6.3.2Organisation Obligations

The obligations of the organisation must be carried out through an authoriser.

The organisation must:

- ensure that their key holders comply with their obligations under this CPS and the CP
- provide measures to avoid compromise of their key holder's private keys
- immediately notify VANguard when the organisation becomes aware that a private key has been compromised, or there is a substantial risk of compromise
- ensure that all information provided to VANguard in relation to issue and use of the key pairs and certificates is to the best of their knowledge, true and complete
- immediately notify VANguard if there is any other change to the registration information, or any other information provided to the RA in relation to issue and use of the keys and certificates
- if requested by the RA, provide complete and accurate registration information or anything else relating to issue or use of the keys and certificates
- where they generate key pairs, comply with Section 6.

The organisation must immediately notify VANguard if:

- any of their key holders cease to be an employee or agent of the organisation
- any of their key holders cease to be authorised to hold keys and certificates on behalf of the organisation
- there is any other change to the Registration Information, or any other information provided to the RA in relation to issue and use of their key holder's keys and certificates.

9.6.3.3Certificate Manager Obligations

The Certificate Manager assumes additional responsibilities in the provisioning of digital certificates.

The Certificate Manager is responsible, on behalf of the organisation, to:

- vouch for the identity of all representatives for whom certificates are requested
- accept responsibility for the use of certificates (through, for example, signature of an SLA)
- accept responsibility for the use of certificates issued to the organisation.

9.6.4 Relying Party Representations and Warranties

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 PDS.

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 relying party or that the certificate is valid.

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 relying party.

The following summarises the recognised parameters under which a digital signature may be relied upon if:

- the signature was created during the operational period of a valid certificate (ie prior to the certificate expiring or being revoked)
- the digital certificate used for signing has the digitalSignature bit asserted in the Key Usage extension
- such digital signature can be properly validated by confirmation of its certificate chain
- the relying party has no notice or knowledge of a breach of the requirements of this CPS or the CP by the signer
- the purpose for which the signature is being relied upon is within the purposes or limitations referred to in the certificate or the CP
- the relying party has complied with all relevant requirements of this CPS.

The use of certificates does not necessarily convey evidence of authority on the part of any user to act on behalf of any person or to undertake any particular act. Relying parties seeking to validate digitally signed messages are solely responsible for exercising due diligence and reasonable judgment before relying on certificates and digital signatures. A certificate is not a grant of any rights or privileges, except as specifically provided in this CPS or this CP.

The relying party is hereby notified of the possibility of theft or other form of compromise of a private key corresponding to a public key contained in a certificate, which may or may not be detected, and of the possibility of use of a stolen or compromised key to forge a digital signature to a document.

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.

9.6.4.1 Digital Signature Validation

Digital signature validation verifies that the digital signature was created by the private key corresponding to the public key listed in the certificate of the relying party named in the certificate (the 'Signer') and that the associated information has not been altered since the digital signature was created. Digital signature validation confirms both the validity of the signer's certificate as well as the digital signature generated using the signer's certificate.

Validation of a digital signature shall be performed by applications to include the following:

- certificate status checking in accordance with Section 4.9.6
- calculate a new hash of the signed information by re-applying the hash function as was originally applied by the Signer
- decrypt the original hash value supplied by the signer by using the public key contained in the certificate
- compare the original hash against the new hash value to confirm that the hash values are equal (equal values denote that the data is unchanged).

9.6.5 Representations and Warranties of Other Participants

9.6.5.1 Repository Obligations

The repository must ensure timely publication of certificates and revocation information as required by this CPS.

See the CP or PDS.

9.7 Disclaimers of Warranties

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 MPKI.

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 PDS and the MOU between VANguard and the relying party.

9.7.1 General Warranty Disclaimer

Except as set forth in this CPS, the CP and the applicable SLA, and to the extent permitted by applicable law, VANguard disclaims any and all express or implied warranties of any type to any person or entity, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided by relying parties.

9.7.2 Specific Disclaimer

Except as otherwise set forth in this CPS, VANguard:

- disclaims all liability to any person or entity arising from the verification (ie proof of identity) of an individual and/or an organisation
- disclaims all liability to any person or entity, regardless of whether the liability arose from negligence, recklessness, fraud, or wilful misconduct, for representations contained in a certificate so long as the certificate was prepared in compliance with this CPS
- does not warrant the standards or performance of any third party hardware or software
- ensures proper verification (ie EOI).

9.7.3 Disclaimer of Fiduciary Relationship

Nothing in this CPS, the CP, or the issuing of key pairs and certificates under it, establishes a fiduciary relationship between VANguard and a relying party.

9.8 Limitations of Liability

The liability of an entity referred to in this CPS for breach of a contract to which the entity is a party, or for any other common law or statutory cause of action, shall be adjudicated according to Sections 9.14 and 9.15 below.

See the CP, PDS, and the MOU between VANguard and the relying party.

Digicert and VANguard limitations of liability are covered in the contract. The provisions set out in this section shall survive the termination of the relevant contract.

9.9 Indemnities

See the PDS and the MOU between VANguard and the relying party.

Digicert and VANguard indemnities are covered in the contract.

9.10 Term and Termination

9.10.1 Term

The provisions of this CPS are in effect once approved by the PAA and published on the Department of Industry, Innovation and Science website.

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

9.10.2 Termination

The Department may terminate the VANguard MPKI at its own discretion, or otherwise as may be required by the Commonwealth government.

The Department will notify relying parties of the intended termination of the VANguard MPKI.

9.10.3 Effect of Termination and Survival

Upon termination VANguard participants are nevertheless bound by the terms of the CP for all certificates issued for the remainder of the validity periods of such certificates. Termination of VANguard shall be conducted in accordance with Section 5.8.

Provisions described as having an ongoing operation survive the termination or expiration of the relevant contractual relationship.

9.11 Individual Notices and Communications with Participants

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

Requests to the VANguard MPKI must be sent to the physical, postal, facsimile or email address as set out on the VANguard website.

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.

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.

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

9.12 Amendments

9.12.1 Procedure for Amendment

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
- a change can only be made to the approved documents once approval has been granted by the PAA
- 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.

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.

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

9.12.2 Notification Mechanism and Period

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.

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

VANguard will inform Digicert 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

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 relying parties. Otherwise where a change to a CPS, CP, or PDS is required, the OID of the policy will stay the same, and this CPS or CP will be provided with a new version number.

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

9.13 Dispute Resolution Provisions

Should a dispute arise between VANguard and Digicert the relevant contract conditions apply.

9.14 Governing Law

This CPS and the CP 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

VANguard agrees to submit to the jurisdiction of the courts having jurisdiction within the Australian Capital Territory, Australia.

9.16 Miscellaneous Provisions

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

9.16.1 Entire Agreement

To the extent of any conflict between the following documents the first mentioned document shall govern:

- the contract between VANguard and PKI entities
- this CPS
- the CP or PDS
- another approved document.

9.16.2 Assignment

See the CP or PDS.

9.16.3 Severability, Survival, Merger

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

9.16.4 Enforcement (Attorney Fees and Waiver of Rights)

See the MOU and SLA entered into between VANguard and a relying party.

9.16.5 Force Majeure

See the PDS and the MOU and SLA entered into between VANguard and a relying party.

9.17 Other Provisions

9.17.1 Conflict of Provisions

To the extent of any conflict between the following documents the first mentioned document shall govern:

- this CPS
- the CP
- the VANguard MOU and SLA
- another agreement between the parties as to the manner and provision of the services described herein
- another approved document
- a document that is not an approved document.