VERISIGN GATEKEEPER CERTIFICATION PRACTICE STATEMENT (VERISIGN GATEKEEPER CPS)

Date of Publication: November 2005
Proposed Effective Date: November 2005

TABLE OF CONTENTS

1. INTRODUCTION

1.0 Structure of this CPS and relationship to Certificate Policy *

1. VeriSign Australia Pty Ltd trading as eSign Gatekeeper Services ('**eSign**') provides both Public and Private certification services using technology from VeriSign Inc.

2. This Certification Practices Statement ("**CPS**") is a general document that sets out a number of policy and operational matters in relation to VeriSign Gatekeeper services, including the practices that VeriSign employs in Issuing, Revoking and managing Certificates. It should be read in conjunction with the relevant Certificate Policy (**"CP"**), which sets out the rules regarding the applicability of a Certificate to a particular community and contains information about the specific structure of the relevant Certificate Type and Grade.

3. The obligations of the PKI Entities are also set out in the relevant VeriSign Gatekeeper CP as well as other relevant documentation including the relevant Subscriber Agreement and Relying Party Agreement.

4. The headings of this CPS follow the framework set out in the Internet Engineering Task Force *Request for Comment 2527* ("**RFC 2527**"). Additional sections or headings have been introduced where necessary for the purposes of this CPS (e.g. this section). These are indicated by an asterisk (*) after the heading.

5. The provisions of the relevant CP prevail over the provisions of the VeriSign Gatekeeper CPS to the extent of any direct inconsistency.

6. Expressions used in this CPS are defined in the Glossary which can be found at the VeriSign Website https://www.verisign.com.au/repository/gatekeeper/.

1.1 Overview

1. VeriSign provides Certification Authority ("CA") and Registration Authority ("RA") services under this CPS and relevant CPs both under its Public Gatekeeper Hierarchy and Private Gatekeeper Hierarchies. Certificates Issued under a Private Hierarchy will not chain to the VeriSign Gatekeeper Root, and allow Agencies to have Certificates issued under varied policies to accommodate their particular requirements.

2. Where VeriSign provides services under a Private Gatekeeper Hierarchy, parts of this CPS may be overridden by the relevant CP in order to address an Agency's particular requirements. VeriSign may also delegate the provision of certain other components of its function for the purposes of Issuance, Verification or Revocation of Certificates and Certificate Applications. The relevant Certificate Policy for the Private Gatekeeper Hierarchy will set out where and to what extent the provisions of the CPS are altered to accommodate the Agency's requirements. All such Certificate Policies for Private Gatekeeper Hierarchies are reviewed and approved for use by the Department of Finance and Administration ("**Finance**").

3. Where VeriSign provides services to a Hosted CA, the Hosted CA will establish its own Certificate Policy that is consistent with this CPS that sets out the policies and procedures that are employed by that organisation in the operation of their Hosted CA. A Hosted CA must be Gatekeeper Accredited as a CA.

Figure 1: VeriSign Public and Private Gatekeeper Hierarchies

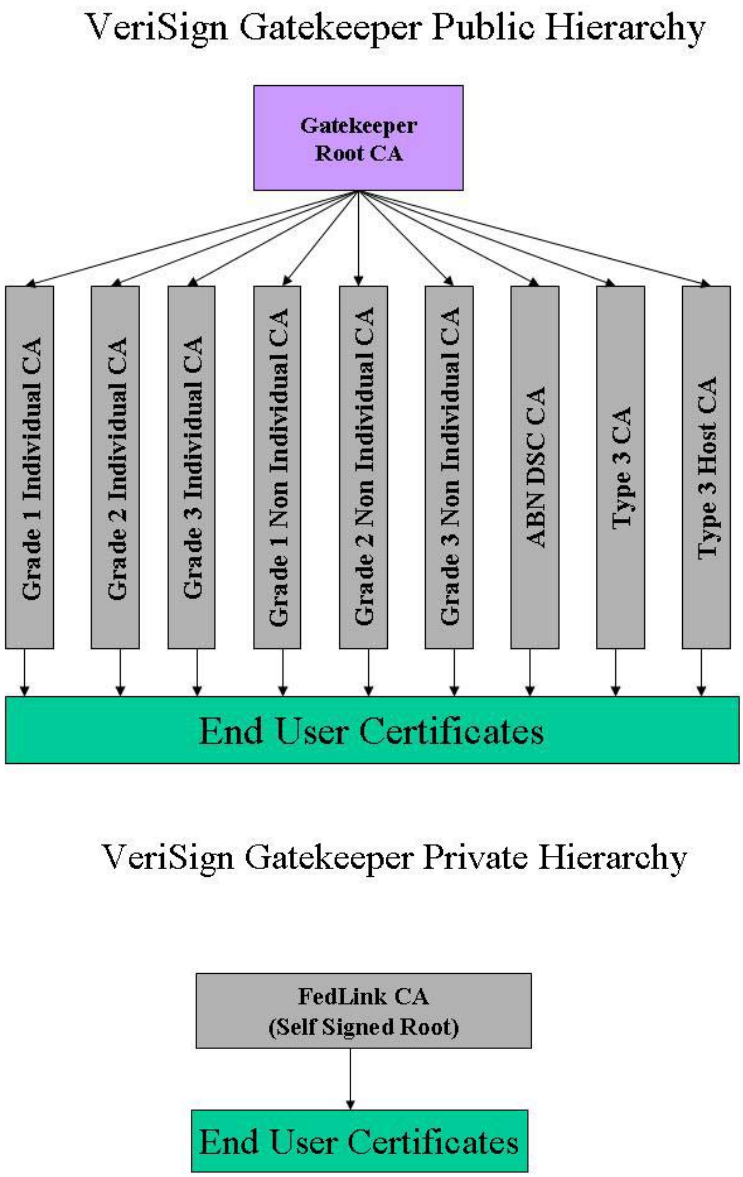
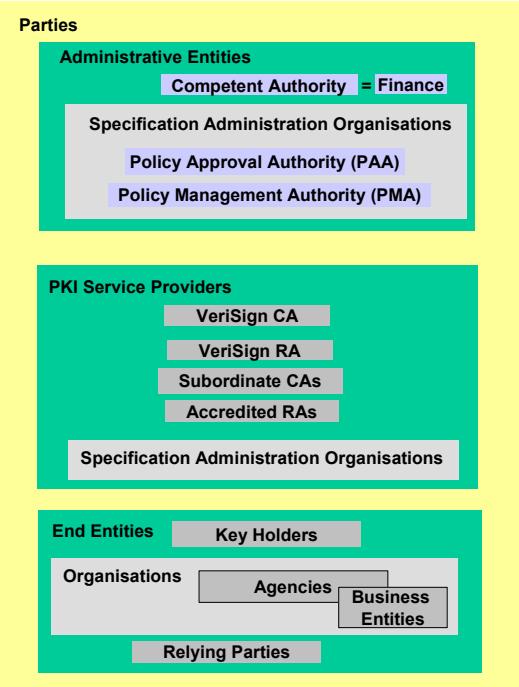


Figure 2: Entities in the Gatekeeper Hierarchy

Entities and Roles



1.2 Identification

The OID for this document is 1.2.36.88088021603.333.1; it is also known as the "VeriSign Gatekeeper CPS".

1.3 Community and applicability

The community of interest for each Certificate is set out in the relevant CP.

1.3.1 Certification Authorities (CAs)

1. Certificates under relevant CPs to which this CPS applies are Issued by the VeriSign Gatekeeper CA, Subordinate CAs and Hosted CAs. The VeriSign CA and Subordinate CAs are operated by VeriSign Australia Pty Ltd. The Certification Authority (CA) that operates Subordinate CAs is the VeriSign CA. Hosted CAs are appointed by VeriSign. They may be managed by an Agency or other organisation but will utilise VeriSign's Gatekeeper Public Key Infrastructure. See further **section 1.1.3**.

2. The Root Certification authority for this CPS is the VeriSign Gatekeeper Root CA ("**VGR**") operated by VeriSign Australia Pty Ltd. The VGR issues Certificates to the VeriSign CA and Subordinate CAs in the VeriSign Gatekeeper Public Hierarchy.

1.3.2 Registration Authorities (RAs)

The VeriSign RA or another Gatekeeper Accredited RA will perform the functions of the Registration Authority. See further the relevant CP.

1.3.3 End Entities

The End Entities to which this CPS applies are Subscribers and Relying Parties as defined in the relevant CP.

1.3.4 Applicability

For restrictions and limitations on the use of different Certificate Types and Grades see the relevant CP.

1.3.5 Gatekeeper Accreditation*

The VeriSign CA has been granted Gatekeeper Accreditation to issue Certificates under this CPS, and perform the other functions specified in this CPS, in accordance with this CPS.

1.4 Contact Details

1.4.1 PKI Service Providers

The current contact details of PKI Service Providers can be found on the VeriSign Gatekeeper Website.

1.4.2 Specification Administration Authorities

The Policy Approval Authority can be contacted as follows:

Attention:	Policy Approval Authority
Physical Address	134 Moray Street, South Melbourne, VIC 3205
Postal Address	PO Box 3092, South Melbourne, VIC 3205
Email	support@verisign.com.au
Facsimile	+61 3 9674 5574

The Policy Management Authority can be contacted as follows:

Attention	Policy Management Authority
Physical Address	134 Moray Street, South Melbourne, VIC 3205
Postal Address	PO Box 3092, South Melbourne, VIC 3205
Email	support@verisign.com.au
Facsimile	+61 3 9674 5574

1.4.3 Contact Person

Enquiries in relation to this CPS should be directed to:

Attention:	Gatekeeper Practices Development
Physical Address	134 Moray Street, South Melbourne, VIC 3205
Postal Address	PO Box 3092, South Melbourne, VIC 3205
Email	support@verisign.com.au
Facsimile	+61 3 9674 5574

1.4.4 Competent Authority

Attention:	Team Leader, Gatekeeper Policy Branch, Australian Government Information Management Office Department of Finance and Administration
Physical Address	Department of Finance and Administration John Gorton Building King Edward Terrace PARKES ACT 2600 AUSTRALIA
Postal Address	As above
Email	gatekeeper@finance.gov.au
Facsimile	+61 2 6215 1659

1.4.5 Person determining CPS suitability for CPs

The Competent Authority will determine that each relevant CP is suitable for use with this CPS. That determination will be set out in this section of each CP.

2. GENERAL PROVISIONS

2.1 Obligations generally*

1. This **section 2.1** sets out important obligations and responsibilities of PKI Entities operating under this CPS.
2. End Entities and any non-VeriSign PKI Service Provider agree not to monitor, interfere with, or reverse engineer the technical implementation of the services provided by the VeriSign CA or the VeriSign RA except as explicitly permitted by this CPS or upon prior written approval from VeriSign.
3. This CPS serves as notice of the rules governing the respective rights and obligations of the PKI Entities among themselves.
4. VeriSign is deemed to have agreed to the CPS on its publication by VeriSign.
5. An entity is deemed to be bound by the provisions of this CPS applicable to a Relying Party when the entity relies on a Certificate issued under this CPS.

2.1.0 RCA Obligations*

1. The root Certification Authority for the purposes of this CPS is the VeriSign Gatekeeper Root (VGR).
2. The VeriSign CA will:
   (a) establish a chain of trust by issuing a Certificate called the VGR which is a self-signed Certificate;
   (b) ensure that the VGR Certificate signs any Subordinate CA Issued under a Public Gatekeeper Hierarchy.

2.1.1 CA obligations

*2.1.1.1 Certificate Issue**

The VeriSign CA or a Subordinate CA which is Issuing a Certificate, will ensure, at the time it Issues a Certificate to a CA that the Certificate contains all the elements required by the Certificate Profile.

*2.1.1.2 Key Management**

1. The VeriSign CA will manage the VeriSign CA Keys in accordance with **section 6**.
2. The VeriSign CA cannot ascertain or enforce any particular Private Key protection requirements of any Organisation or Subscriber. See further **section 6**.

*2.1.1.3 Directories and Certificate Revocation**

The VeriSign CA will:

(a) ensure the availability of a Certificate Directory and CRL as required under **section 2.6**; and
(b) promptly Revoke a Certificate if required under **section 4.4**;
(c) ensure that the date and time when a Certificate is Issued or Revoked can be determined precisely.

*2.1.1.4 General**

The VeriSign CA will:

(a) 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;
(b) apply administrative and management procedures which are appropriate for the activities being carried out;
(c) use Trustworthy Systems and Evaluated Products which are protected against modification, and ensure the technical and Cryptographic security of the process supported by them; and

(d) 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.

*2.1.1.5 Obligations of Subordinate CAs**

Subordinate CAs must meet all the CA obligations set out in **section 2.1.1**.

2.1.2 RA Obligations

No RA functions are performed under this CPS. See the relevant CP for details about the RA function performed before Certificates are issued to End Entities.

2.1.3 Subscriber Obligations

See the Relevant CP.

2.1.4 Relying Party obligations

1. Before relying on a Certificate or a Digital Signature, Relying Parties must:

   (a) Validate the Certificate and Digital Signature (including by checking whether or not it has been Revoked, Expired or Suspended) in accordance with **section 2.1.4.1**; and

   (b) 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, the relevant CP or this CPS.

2. If a Relying Party relies on a Digital Signature or Certificate in circumstances where it has not been Validated in accordance with **section 2.1.4.1** it assumes all risks with regard to it (except those that would have arisen had the Relying Party Validated the Certificate) and is not entitled to any presumption that the Digital Signature is effective as the signature of the Subscriber or that the Certificate is valid.

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

2.1.4.1 Validating Digital Signatures*

1. Validation of a Digital Signature is undertaken to determine that:

   (a) the Digital Signature was created by the Private Key Corresponding to the Public Key listed in the Certificate of the person affixing their Digital Signature to the information (the '**Signer**'); and

   (b) that the associated information has not been altered since the Digital Signature was created.

2. Validation of a Digital Signature is performed by applications following this process:

   (a) **Establishing a Certificate Chain for the Certificate used to sign the information** – In the case of a Public Hierarchy this involves confirming that the CA who Issued the Certificate is a Subordinate CA of the VGR. In the case of a Private Hierarchy it involves confirming that the CA who issued the Certificate is trusted by the Relying Party;

   (b) **Checking the Repository for Revocation of Certificates in this Chain** – The Relying Party must determine if any of the Certificates along the chain from the Signer to an acceptable root within the VeriSign Gatekeeper PKI have been Revoked, because a Revocation has the effect of prematurely terminating the Operational Period during which verifiable Digital Signatures can be created. This may be ascertained by querying the CRL or OCSP responder (if available) to determine whether any Certificates in the Certificate Chain have been Revoked;

   (c) **Applying the hash function to the signed data** – Apply the same hash function as was originally applied by the Signer;

   (d) **Decrypting the original hash** – Using the Public Key contained in the Certificate decrypt the original hash value; and

   (e) **Compare the hash functions** – If the value created by step 2(c) is the same as the value recovered by step 2(d), then the information is Validated.

3. A PKI Entity agrees that a Digital Signature may be relied upon against the Signer if:

   (a) it was created during the Operational Period of a valid Certificate (ie before the Certificate Expired or was Revoked);

(b) the Digital Certificate used for Signing has the digitalSignature Bit asserted in the Key Usage extension;

(c) such Digital Signature can be properly Validated by confirmation of its Certificate Chain;

(d) the Relying Party has no knowledge or notice of a breach of the requirements of the relevant CP or this CPS by the Signer;

(e) the purpose for which it was relied on was within the purposes or limitations referred to in the Certificate or the relevant Certificate Policy;

(f) the Relying Party has no knowledge of a reason why the Digital Signature should not be relied upon in the circumstances; and

(g) 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 A 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 FROM VERISIGN OF ANY RIGHTS OR PRIVILEGES, EXCEPT AS SPECIFICALLY PROVIDED IN THE RELEVANT CPS OR THIS CPS.

YOU ARE 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. FOR INFORMATION REGARDING PRIVATE KEY PROTECTION, SEE THE VERISIGN GATEKEEPER WEBSITE.

4. Additionally, the Relying Party should consider the Certificate Grade. The final decision concerning whether or not to rely on a verified Digital Signature is exclusively that of the Relying Party.

2.1.5 Repository Obligations

An entity operating a repository must ensure timely publication of Certificates and Revocation information as required by this CPS.

2.2 Liability[1]

2.2.1 Liability Generally*

1. 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 determined under the relevant law in Australia that is recognised, and would be applied, by the High Court of Australia.

2. Where a PKI Entity is legally liable to compensate another party, the liability of the first mentioned PKI Entity will be reduced proportionally to the extent that any act or omission on the part of the other PKI Entity contributed to the relevant liability, loss, damage, cost or expense.

3. The PKI Entities acknowledge that one of the factors that affects their ability to limit their liability is the extent to which they effectively notify the PKI Entity suffering the loss or damage of any limits or limitations on which the entity intends to rely.

4. The provisions set out in this **section 2.2** survive the termination of the relevant contract.

5. Apart from **section 2.2.2**, the liability regime applicable to activities conducted under this CPS by the VeriSign CA or the VeriSign RA is not evaluated by a member of the Gatekeeper Legal Panel, nor is it approved by the Competent Authority.

2.2.2 Liability of the Commonwealth*

1. The Competent Authority is only responsible for performing the accreditation process with due care, in adherence to published Gatekeeper Criteria and Policies. The Competent Authority is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Certification or Registration Authority as the case may be.

2. Notwithstanding any other provisions of this CP:

[1] The sections of heading 2.2 have been significantly expanded from RFC2527.

(a) the Commonwealth makes no representations, and offers no warranties or conditions, express or implied, in relation to:

(i) the activities or performance of any of the PKI Service Providers which are carried out under, or in relation to, this CP; or

(ii) if relevant, the services or products of a particular PKI Service Providers; and

(b) the PKI Entities acknowledge and agree that except to the extent that a Commonwealth Agency is carrying out the role of a PKI Entity (in which case the liability of the Commonwealth will be determined in accordance with the provisions set out in this **section 2.2**), the Commonwealth is not liable in any manner whatsoever whether the Keys or Certificates are used in a transaction with an Agency or not, for any loss or damage caused to, or suffered by any person, including a PKI Entity as a result of:

(i) an entity described in this CP carrying out, or omitting to carry out, any activity described in, or contemplated by, the Approved Documents;

(ii) the Commonwealth carrying out, or omitting to carry out, any activity related to the Gatekeeper accreditation process;

(iii) a negligent act or omission of the Commonwealth.

2.2.3 Force majeure*

1. A PKI Entity is not liable for any loss or damage arising from any delay or failure to perform its obligations described in the relevant CP or this CPS if such delay is due to Force Majeure.

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

3. If delay or failure by a PKI Service Provider to perform its obligations due to Force Majeure exceeds 30 days, the PKI Entity affected by the failure to perform the obligations may terminate the arrangement, agreement or contract it has with the non-performing PKI Service Provider on providing notice to that PKI Entity in accordance with this CPS. If the arrangement, agreement or contract is terminated, then the non-performing PKI Service Provider shall refund any money (if any) paid by the terminating entity to the non-performing entity for services not provided by the non-performing PKI Service Provider.

2.2.4 VeriSign Liability*

1. VeriSign and the Relevant RA exclude all warranties, conditions and obligations of any type from the relationship between VeriSign or the Relevant RA and any other PKI Entity (including without limitation as a result of operating the VeriSign CA or the VeriSign RA or the VGR) except:

(a) to the extent otherwise provided in this CPS; or

(b) where a condition or warranty is implied into an agreement by a law, and that condition or warranty cannot be excluded.

2. In no event will VeriSign or the Relevant RA be liable for any indirect, special, incidental, or consequential damages or for any loss of profits or revenues, loss of data, loss of use, loss of goodwill, or other indirect, consequential, or punitive damages, whether or not reasonably foreseeable, arising from or in connection with the use, delivery, license, performance, or non-performance of Certificates, Digital Signatures, or any other transaction or services related to or offered or contemplated by the relevant CP or this CPS, breach of contract or any express or implied warranty or indemnity under or in relation to any Certificates or the relevant CP or this CPS or otherwise misrepresentation, negligence, strict liability or other tort, even if VeriSign or the Relevant RA has been advised of the possibility of such damages or should have been aware of such a possibility.

3. VeriSign's and the Relevant RA's aggregate liability to a non-VeriSign PKI Entity and any and all persons concerning a Certificate for the aggregate of all Digital Signatures and transactions related to that Certificate, shall be limited to AUD 50,000.

4. In the event that VeriSign's or the Relevant RA's total liability exceeds the amount above, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall VeriSign or the Relevant RA be obligated to pay more than the aggregate liability cap for each Certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

5. In regard to **section 2.2.4** VeriSign is also contracting as an agent for Australia Post. Subscribers and Relying Parties agree that they have not relied on any warranty or representation by Australia Post in entering the Subscriber Agreement or the Relying Party Agreement.

2.2.5 Subscriber Liability*

See the relevant CP.

2.2.6 Relying Party Liability

No stipulation.

2.3 Financial responsibility

2.3.1 Indemnification of Relying Parties

No stipulation.

2.3.2 Fiduciary relationships

Nothing in the relevant CP, this CPS, or the issuing of Key Pairs and Certificates under it, establishes a fiduciary relationship between a PKI Service Provider and an End Entity.

2.3.3 Administrative processes

VeriSign's financial viability was examined before it was granted endorsement under the Endorsed Supplier Arrangements.

2.4 Interpretation and Enforcement

2.4.1 Governing law

1. The relevant CP and this CPS 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.
2. The PKI Entities agree to submit to the jurisdiction of the courts having jurisdiction within the Australian Capital Territory, Australia.

2.4.2 Severability, survival, merger, notice

*2.4.2.1 Severability**

Any reading down or severance of a particular provision does not affect the other provisions of the relevant CP or this CPS.

*2.4.2.2 Survival**

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

*2.4.2.3 Notice**

1. Notices to Subscribers must be sent to the physical, postal, facsimile or email address of the Subscriber, which is included in its Registration Information, or to another address which the Subscriber has specified to the sender.
2. Notices to a PKI Service Provider must be sent to the physical, postal, facsimile or e-mail address of that entity set out on the VeriSign Website, or to another address which the entity has specified to the sender.
3. A notice to any entity in relation to this CPS must be signed by the sending entity. If the notice is sent electronically it must be digitally signed.
4. A notice sent is taken to be received:
   (a) if it is hand-delivered to a physical address - at the time of delivery whether or not any person is there to receive it;
   (b) 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;
   (c) if it is transmitted by facsimile - when the sending machine produces a report showing the transmission was successful; and
   (d) if it is sent by e-mail - when it enters a system under the control of the addressee.

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

*2.4.2.4 Precedence**

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

(a) the relevant CP;

(b) this CPS;

(c) the applicable Subscriber Agreement;

(d) another agreement between the parties as to the manner and provision of the services described herein;

(e) another Approved Document; and

(f) a document that is not an Approved Document.

2.4.3 Dispute resolution procedures

1. If a dispute arises between any PKI Entity (**Dispute**), either PKI Entity to the Dispute may by written notice to the other PKI Entity specify the details of the Dispute (**Dispute Notice**).
2. If a Dispute Notice is given, then the PKI Entity must promptly meet and negotiate in good faith to resolve the Dispute.
3. If the Dispute remains unresolved 30 days after receipt of the Dispute Notice, the PKI Entities agree to submit the Dispute to mediation administered by, and in accordance with, the mediation rules of the Australian Commercial Disputes Centre (**ACDC**). A single mediator will be agreed by the PKI Entities or, failing agreement, appointed by the ACDC. The Mediation will be held in Melbourne and be subject to the laws in force in the Australian Capital Territory, Australia.
4. This **section 2.4.3** does not apply where both PKI Entities to the dispute are Agencies.
5. A PKI Entity may be legally represented in any mediation.
6. The VeriSign CA must notify the Competent Authority before commencing legal proceedings against any Subscriber where the VeriSign CA is aware that Keys and Certificates have been issued to the Subscriber for the purpose of facilitating electronic transactions with an Agency.
7. Nothing in this **section 2.4.3** prevents a PKI Entity from seeking urgent equitable relief before an appropriate Court.

2.5 Fees

See the relevant CP. The VeriSign CA's fees for Certificates and related services can be obtained from the VeriSign Gatekeeper Website.

2.5.1 Certificate Issuance or Renewal fees

The VeriSign CA's fees for Certificates and related services can be obtained from the Gatekeeper Website.

2.5.2 Certificate access fee

Certificates are published in the Directory. There is no additional fee for accessing Certificates.

2.5.3 Revocation or status information access fee

Revocation status is published in the CRL. There is no additional fee for accessing the CRL.

2.5.4 Fees for other services such as policy information

Fees for other VeriSign services can be obtained from the VeriSign Gatekeeper Website.

2.5.5 Refund Policy

There is a charge per Certificate Issued. Once a Certificate is Issued, a refund will not be provided. The VeriSign CA will Issue a new Certificate free of charge if, through the fault of the VeriSign CA, the VeriSign CA erroneously Issued a Certificate.

2.6 Publication and Repository

See the relevant CP for details regarding publication of documents and the Repository.

2.6.1 Publication of CA information

1. The VeriSign CA must make the VGR Certificate and the VGR Public Key reasonably available to End Entities.
2. The VeriSign CA must properly maintain the VeriSign Gatekeeper Website at which it publishes or links to:
   (a) the Repository;
   (b) the Certificate Directory;
   (c) the Certificate Revocation List (CRL);
   (d) the CPs;
   (e) this CPS; and
   (f) other Approved Documents (excluding those which are not publicly available – see the definition of Approved Documents in the Glossary).

2.6.2 Frequency of publication

1. The VeriSign CA will update the Certificate Directory as soon as practicable whenever a new Certificate is Issued.
2. The VeriSign CA will update the CRL at least daily.
3. Where available for that particular Certificate Type, the OCSP responder provides real time Certificate Revocation status.

2.6.3 Access controls

1. There are no controls on read-only access to this CPS, and other Approved Document (see definition of 'Approved Documents' in the Glossary).
2. Access to the Certificate Directory and the CRL is limited to single searches on the following fields as defined in the relevant Certificate Profile: Version; Serial Number; Signature; Issuer; Validity; Subject; Subject Public Key Information; Issuer Unique Identifier; Subject Unique Identifier; and Extensions.

2.6.4 Repositories

The functions of the VeriSign CA under **sections 2.6.1 to 2.6.3** (inclusive) may be performed on the VeriSign CA's behalf by a third party repository.

2.7 Compliance audit

2.7.1 Frequency of entity compliance audit

The VeriSign CA and the VeriSign RA will be audited annually, or more frequently if required, by an authorised auditor from the panel of Gatekeeper authorised auditors.

2.7.2 Identity/qualifications of auditor

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 Gatekeeper CA and RA Accreditation Criteria.

2.7.3 Auditor's relationship to audited party

Gatekeeper auditors will be independent of the audited entity.

2.7.4 Topics covered by audit

The purpose of Gatekeeper audits is to ensure that the VeriSign CA and VeriSign RA:

(a) maintains compliance with Gatekeeper Accreditation criteria and policies; and

(b) continues to operate as required by the Approved Documents.

2.7.5 Actions taken as a result of deficiency

1. Actions recommended by the auditor arising from any deficiency revealed by a Gatekeeper audit will be discussed by the audited entity and authorised representatives of Finance. If necessary, the Competent Authority may direct the audited entity to take certain remedial action.

2. Failure to adequately address deficiencies identified in an audit may result in withdrawal of the entity's Gatekeeper Accreditation.

2.7.6 Communication of results

1. The date on which the VeriSign CA or VeriSign RA was last audited will be published on the VeriSign Gatekeeper Website and may also be published by Finance.

2. The results of a Gatekeeper audit are confidential and will be communicated by the auditor only to authorised representatives of Finance and the audited entity. Results of the compliance audit of the VeriSign CA and RA operations may be released at the discretion of VeriSign management.

2.8 Privacy and Data Protection

See the relevant CP for details regarding the treatment of confidential information.

2.9 Intellectual Property Rights

See the relevant CP for details regarding intellectual property rights.

3. IDENTIFICATION AND AUTHENTICATION

See the relevant CP for information regarding initial registration, Renewal, Reissue and Revocation of Certificates.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

See the relevant CP.

4.2 Certificate issuance

See the relevant CP.

4.3 Certificate acceptance

See the relevant CP.

4.4 Certificate Suspension and Revocation

See the relevant CP.

4.5 Security Audit Procedures

The Protective Security Plan addresses event logging and audit systems which are implemented for the purpose of maintaining a secure environment.

4.5.1 Type of event recorded

The following events are recorded in audit log files:

- System start-up and shutdown
- CA/RA application start-up and shutdown
- Attempts to create, remove or set passwords or change the system privileges of users performing Trusted Roles
- Changes to CA/RA details and/or keys
- Login and logoff attempts
- Unauthorised attempts to gain access to the network of the CA/RA system
- Generation of own and subordinate CA/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 Subscribers.

4.5.2 Frequency of processing log

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

4.5.3 Retention period for audit log

Audit logs shall be retained for at least two months after processing and thereafter archived.

4.5.4 Protection of audit log

Electronic audit logs are protected against unauthorised viewing, modification, deletion and other tampering by storage within a Trustworthy System.

4.5.5 Audit log backup procedures

Electronic audit logs are fully backed up weekly, with incremental backups performed daily.

4.5.6 Audit collection system (internal vs external)

The audit system is maintained internally.

4.5.7 Notification to event-causing subject

The event causing subject will not necessarily be notified of the occurrence of an audit event. Notification will be performed where the VeriSign CA believes it is necessary in the circumstances.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

1. The Protective Security Plan includes general records archival and records retention policies.
2. The VeriSign CA and PKI Service Providers shall maintain records in a trustworthy fashion, including documentation of actions and information that is material to each Certificate Application and to its creation. These records shall include all relevant evidence in their possession regarding:
   - the identity of the Applicant named in each Certificate;
   - the identity of persons requesting Certificate Revocation;
   - other facts represented in the Certificate;
   - Time Stamps; and
   - any other material facts related to issuing Certificates.
3. PKI Service Providers must make available to the VeriSign CA any information held by them under this section, subject to any privacy obligations they may be subject to.
4. Records may be kept in the form of either computer based information or paper based documents, provided their indexing, storage, preservation, and reproduction are accurate, secure and complete.

4.6.1 Types of event recorded

Most of the information collected by the VeriSign RA is archived including the records referred to in **section 4.6**.

4.6.2 Retention period for archive

Records are retained in relation to Certificates (including Personal Information) for at least 30 years after the date the Certificate Expires or is Revoked.

4.6.3 Protection of archive

Only Trusted Employees are able to access the archive. Archived records are protected against unauthorised viewing, modification, deletion and other tampering by storage within a Trustworthy System.

4.6.4 Archive backup procedures

Electronic archives are fully backed up weekly, with incremental backups performed daily.

4.6.5 Requirements for Time Stamping of records

The following records are Time Stamped:

- Certificates
- CRLs and other Revocation databases
- Customer service messages.

4.6.6 Archive collection system (internal or external)

The archive collection system is maintained internally.

4.6.7 Procedure to obtain and Verify archive information

On request and subject to the other provisions in this CPS including in relation to confidentiality and Personal Information, the VeriSign CA can provide access to archived information.

4.7 Key changeover

1. Key changeover is where after expiry of a CA Key, the Subscriber needs to obtain new CA Keys (and CA Certificates). The process is dealt with in the section covering Renewals.

2. Key changeover for Subordinate CAs involves the VeriSign CA confirming the identity of the Subordinate CA and performing a Key generation ceremony after which the Subordinate CA's Key Pair is replaced with the new Key Pair.

4.8 Compromise and Disaster Recovery

1. The VeriSign CA maintains a Disaster Recovery and Business Continuity Plan covering all reasonably foreseeable types of disasters and compromises affecting the services under this CPS including:

   (a) loss or corruption (including suspected corruption) of computing resources, software, and/or data of the VeriSign CA or another PKI Service Provider; and

   (b) Compromise of the VeriSign CA's Private Keys which Relying Parties rely on to establish trust in Certificates.

2. The Disaster Recovery and Business Continuity Plan are consistent with the requirements of the VeriSign CA's Protective Security Plan. For security reasons these plans are not publicly available.

4.8.1 Computing resources, software, and/or data are corrupted

If computing resources, software and/or data are corrupted, the processes outlined in the Disaster Recovery and Business Continuity Plan will be performed.

4.8.2 Entity Public Key is Revoked

If a Key Pair of the VeriSign CA is Revoked (including as a result of Compromise), the Revocation shall be reported in the CRL and in the Repository.

4.8.3 Entity Key is Compromised

If a Subordinate CA's Private Key is Compromised, the VGR will Revoke the CA's Certificate, and report that fact in accordance with **section 4.8.2**.

4.8.4 Secure facility after a natural or other type of disaster

The Disaster Recovery and Business Continuity Plan sets out response and recovery procedures for each type of disaster or Compromise.

4.9 PKI Service Provider Termination*

1. This **section 4.9** applies if the VeriSign CA becomes aware that it or another PKI Service Provider intends to, or is likely to, cease providing services, which are:

   (a) necessary for Issue of Keys and Certificates under this CPS; or

   (b) necessary for reliance on Digital Signatures or Certificates.

2. The VeriSign CA will give as much notice as possible of the relevant circumstances, and the actions the VeriSign CA proposes to take to:

(a) the Competent Authority;

(b) all Subscribers; and

(c) the Relying Parties of which the VeriSign CA is aware;

in this **section 4.9** referred to as the 'affected parties'.

3. In the circumstances described in **section 4.9.1**, each PKI Service Provider must co-operate with each other in minimising disruption to the services provided under this CPS and to the affected parties.

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

5. If a PKI Service Provider (including the VeriSign CA itself) unexpectedly ceases providing services referred to above, the VeriSign CA must immediately give notice to the affected parties.

6. If any Personal Information is transferred from one PKI Service Provider to another, each relevant PKI Service Provider must ensure that the information is protected as required under **section 2.8**.

7. The obligations under this **section 4.9** are in addition to any obligations the VeriSign CA or any other entity has under the requirements of **section 4.8**.

8. The termination of a non-VeriSign Subordinate CA is subject to the contract entered into between the owner of that CA and VeriSign. VeriSign and the owner shall use commercially reasonable efforts to agree on a termination plan that minimises disruption to customers, Subscribers and Relying Parties. The termination plan should cover such issues as:

(a) providing notice to the affected parties such as Subscribers and Relying Parties;

(b) who bears the cost of such notice;

(c) the Revocation of the Certificate issued to a Subordinate CA;

(d) the preservation of the Subordinate CA's archives and records for the time periods required in **section 4.6** of the CPS;

(e) the continuation of Subscriber and customer support services;

(f) the continuation of Revocation services, such as the Issuance of CRLs or the maintenance of OCSP; and

(g) the Revocation of Certificates, if necessary.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.0 General*

5.0.1 Security Policy*

The VeriSign CA's Protective Security Plan states the manner and type of protection for the VeriSign CA's system and information, including in relation to:

(a) Confidentiality – who is allowed to see the information to be processed, the system documentation, software, or any other aspect of the system;

(b) Integrity – who is allowed to change the information, the system documentation, software or any other aspect of the system; and

(c) Availability - how important it is that the system should be available to users at any given time.

5.0.2 Protective Security Risk Review*

1. DSD has, at the commencement of the VeriSign CA's operations, evaluated VeriSign's Protective Security Risk Review (PSRR) and confirmed that the PSRR meets the criteria of Australian/New Zealand Standard AS/NZS 4360. For Gatekeeper Accreditation, the PSRR is evaluated against the following, which meet or exceed the criteria of Australian/New Zealand Standard AS/NZS 4360:

(a) Australian Government Information and Communications Technology Security Manual (ACSI 33);

(b) the Defence Signals Directorate Criteria for Accreditation of Certification Authorities - Supplementary Information for Criteria SE01, SE02, SE04, SE05A, SE05B, PE02.

2. The VeriSign CA maintains a configuration management program to update the PSRR in response to changes to the VeriSign CA's or RA's operations.

5.0.3 Protective Security Plan*

1. The VeriSign CA maintains a Protective Security Plan which describes the practices for ensuring the security and integrity of the overall operation of the VeriSign CA, including the establishment of standards for the access and operation of the VeriSign CA's service elements. The Protective Security Plan was evaluated against the same documents as are set out in **section 5.0.2**.

2. The Protective Security Plan details those procedures which are necessary to ensure that the VeriSign CA's clients can have the highest possible level of assurance that critical functions have been identified, and have been provided at appropriate levels of trust, in particular, CA Private Key security, key/data recovery (ie. lost keys or legal access), privileged user management, Certificate publication and integrity, key generation and transfer mechanisms.

3. The Protective Security Plan includes the following elements: System Description; Security Objectives; Data Description; System Users; System Mode; Security Administration; Physical Security to Highly Protected level; Comsec (Communications Security) Standards; Networking; Logical Access Control; Audit Accountability; Quality Assurance; Configuration Management; System Integrity; Contingency Handling; Education and Training; Control of Removable Media; Maintenance, Sanitising and Disposal of Hardware and Software; Data Transfer Procedures; Emergency Destruction; and Incident Management.

4. Many of the documents referred to above are not publicly available and therefore their contents are not detailed in this document.

5.1 Physical Controls

The Protective Security Plan details the physical controls on the facilities housing the VeriSign CA's systems, including in relation to: 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; and Intruder detection systems.

5.1.1 Site location and construction

VeriSign's Regional Operations Centre has been designed to provide a physically protected environment that deters, detects and prevents unauthorised use of, access to, and disclosure of sensitive information and systems. The security of the centre has been reviewed by a member of the Gatekeeper Physical Security Evaluation Panel. as part of the accreditation process.

5.1.2 Physical access

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

5.1.3 Power and air conditioning

The regional operations centre has its backup diesel generator on site as a fail-safe power supply in the event of power failure. This generator provides power on a priority basis to key services and areas.

5.1.4 Water exposures

The regional operations centre is constructed to prevent floods and water damage.

5.1.5 Fire prevention and protection

The regional operations centre is constructed and equipped to prevent and extinguish fire damage

5.1.6 Media storage

Media is stored in a manner to prevent information being used or accessed by unauthorised personnel including by storing such material in appropriate security containers for the classification level of the media held.

5.1.7 Waste disposal

Records containing Personal Information are destroyed in a manner to prevent the unauthorised access to information. Shredders are available throughout the facility.

5.1.8 Off-site backup

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

5.2 Procedural Controls

5.2.1 Trusted roles

Positions of Trust are identified in the Trusted Employee Policy as are the procedures that are implemented to ensure that appropriate screening is performed of these people. The screening performed on individuals occupying Positions of Trust varies with the duties they must perform. People having access to Personal Information are cleared to Highly Protected in accordance with Gatekeeper requirements.

5.2.2 Number of persons required per task

All Cryptographic activity takes place in the presence of two or more trusted employees who have been authorised for the purpose.

5.2.3 Identification and authentication for each role

The Protective Security Plan specifies identification and authentication requirements, which must be met before a person can perform the roles and functions of a Position of Trust.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

1. All VeriSign CA staff occupy a Position of Trust and are vetted through a process described in the Trusted Employee Policy. Positions that require Highly Protected status are specified in the Trusted Employee Policy.
2. The VeriSign CA has established and maintains a position of Facility Security Officer.

5.3.2 Background check procedures

Background checks for security clearance to the level of Highly Protected are carried out in accordance with the Gatekeeper requirements.

5.3.3 Training requirements

Requirements for training of VeriSign staff are set out in the relevant Operations Manual.

5.3.4 Retraining frequency and requirements

Staff are provided with refresher training to the extent and frequency required to ensure that they 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.

5.3.6 Sanctions for unauthorised actions

The Trusted Employee Policy and VeriSign's employee handbook set out appropriate sanctions for unauthorised actions by VeriSign and other staff.

5.3.7 Contracting personnel requirements

Section 5.3 applies to a person within VeriSign's operations notwithstanding that they are a contractor.

5.3.8 Documentation supplied to personnel

All VeriSign staff are made aware of the requirements of the Approved Documents that are relevant to their duties. This includes an acknowledgement by VeriSign staff that they will comply with the Employee Handbook and retain a Trusted Employee status.

6. TECHNICAL SECURITY CONTROLS

6.0 Key Management*

1. The CP deals with the generation and distribution of Keys for Subscribers.

2. The VeriSign CA maintains the Key Management Plan, which specifies technical security controls on generation, distribution and use of its own CA Key Pairs. The VeriSign CA's Key Pairs are generated using algorithms that comply with the standards described in the Gatekeeper Report, Annex H 'Security Standards'.

3. The Key Management Plan also addresses the responsibilities of the VeriSign CA, and each Subordinate Entity against each of the items under **sections 6.1, 6.2 and 6.3;** accordingly only summary details are contained below.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair generation

1. Key Pair generation shall be performed using Trustworthy Systems and processes that provide the required Cryptographic strength of the generated Keys, and prevent the loss, disclosure, modification, or unauthorised use of such Keys.

2. Key Pair generation performed by the VeriSign CA (eg for generation of CA Keys) will be performed in accordance with the Key Management Plan.

6.1.2 Private Key delivery to Entity

The VeriSign CA does not deliver its CA Private Keys to any entity.

6.1.3 Public Key Delivery to Certificate Issuer

See **section 6.1.4.**

6.1.4 VeriSign CA Public Key delivery to users

1. The VeriSign CA's Public Key or the Public Keys of Subordinate CAs are delivered to the Subscriber as part of the process of Issuance of a Certificate to a Subscriber, in an online transfer meeting the IETF RFC 2510 (PKI Certificate Management Protocols) standard using Evaluated Products, or equally secure non-electronic means.

2. The VGR CA's Public Key, and the Public Keys of all Subordinate CAs, will be made available to download in the Repository.

6.1.5 Key sizes

1. The VeriSign CA's Keys are 1024 bits or longer.

2. The VGR Keys are 2048 bits long. A trustworthy hardware device operating within a processing centre is used to create, protect, and store the VGR's Private Key.

3. Each Subordinate CA's key size is 1024 bits. A trustworthy hardware device operating within a processing centre is used to create, protect, and store each Subordinate CA's Private Keys.

6.1.6 Public Key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software Key generation

The VeriSign CA's Key Pairs are generated by a hardware device.

6.1.9 Key usage purposes (as per X.509 v 3 Key Usage field)

Key usage is defined in accordance with that described in X.509 version 3. See the relevant CP for specific details on restrictions imposed using the key usage field.

6.2. Private Key Protection

The VeriSign CA uses mechanisms detailed in the Key Management Plan to protect its Private Keys from loss, disclosure, modification or unauthorised use.

6.2.1 Standards for Cryptographic Module

VeriSign maintains and uses Industry standard specialised Cryptographic Hardware modules. .

6.2.2 Private key (n out of m) multi-person control

The VeriSign CA uses Multi Person Control for the VeriSign CA Keys where there is a risk that the integrity of the PKI could be compromised by misuse of the Key.

6.2.3 Private Key Escrow

The VeriSign CA does not Escrow its CA Private Keys although it does back them up.

6.2.4 Private Key backup

The VeriSign CA backs up the Private Keys of its CAs and these backups are stored in the VeriSign CA's secure facility and an external secure location for the purposes of data recovery.

6.2.5 Private Key archival

The VeriSign CA keeps a copy of all Private Keys it has historically used.

6.2.6 Private Key entry into Cryptographic Module

The specifics of how the VeriSign CA manages its Private Keys and how these are stored in Cryptographic Modules is sensitive information and is not publicly available.

6.2.7 Method of activating Private Key

See **section 6.2.6** above.

6.2.8 Method of deactivating Private Key

When a VeriSign CA is taken offline, the token containing the CA's Private Key will be removed from the reader in order to deactivate it.

6.2.9 Method of destroying Private Key

Private Keys will be destroyed in a way that prevents their loss, theft, modification, unauthorised disclosure, or unauthorised use.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key archival

The VeriSign CA archives the Public Keys of its CAs and the archived Public Keys can be found in the Repository.

6.3.2 Usage periods for the Public and Private Keys

Figure 3: Key Pair Operational Period

Key Pair	Operational Period
VeriSign Gatekeeper Root CA 's Key Pair	To 24 May 2014
VeriSign ABN-DSC CA Key Pair	To 24 May 2012
VeriSign Individual and Non-Individual CAs' Key Pairs	To 24 May 2012
VeriSign Type 3 CA	To 10 April 2013
VeriSign Type 3 Host CA	To 24 May 2012
VeriSign Private Hierarchy CA	To 12 September 2011

PKI Entities shall cease all use of their Authentication (Signing) Private Key after their usage periods have Expired.

6.4 Activation Data

See the relevant CP.

6.5 Computer Security Controls

1. The Protective Security Risk Review covers security of the VeriSign CA's operations and systems used to provide computer security.

2. All PKI Service Providers shall utilise only Trustworthy Systems in performing their respective services.

6.5.1 Specific computer security technical requirements

Systems that operate the CA software and store data files use Trustworthy Systems to secure against unauthorised access. Production servers used to support Gatekeeper Certificates operate on their own hardware and software platform and are not generally accessible or available for other uses.

6.5.2 Computer security rating

See **section 6.5.1.**

6.6 Life Cycle Technical Controls

The details of the VeriSign CA's life cycle technical controls is sensitive information and is not detailed in this document.

6.6.1 System development controls

See **section 6.6.**

6.6.2 Security management controls

See **section 6.6**.

6.6.3 Life cycle security ratings

No stipulation.

6.7 Network Security Controls

These are specified in the Protective Security Plan and Protective Security Risk Review. In general, the VeriSign 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.

6.8 Cryptographic Module Engineering Controls

See **section 6.2.1**.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

The relevant CP contains the Certificate Profile for End Entity Certificates. The section below explains the Certificate Profile for the VGR, and other VeriSign CAs.

Table 1: Certificate Profile of VeriSign Gatekeeper Root

Type	Value
Subject (Distinguished Name)	CN = Gatekeeper Root CA OU = Gatekeeper PKI O = eSign Australia
Issuer (Distinguished Name)	CN = Gatekeeper Root CA OU = Gatekeeper PKI O = eSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	RSA 2048 bit key
Valid From	Dd/mm/yy hh/mm/ss
Valid To	Dd/mm/yy hh/mm/ss
Basic Constraints	CA: Set; Max Path Len: 8
Key Usage	CertSign CRLSign
Netscape Cert Type	OID 2.16.840.1.113730.1.1 Value 03 02 07 80
Subject Key Identifier	Set (sha1 hash of Public Key)
Authority Key	Set (sha1 hash of issuer's Public Key)

Identifier	
Thumbprint algorithm	sha1
Thumbprint	Thumbprint value

Table 2: Certificate Profile of ABN-DSC CA

Type	Value
Subject (Distinguished Name)	CN = eSign ABN DSC CA OU = Terms of use at https://www.esign.com.au/GKRPA/ OU = Gatekeeper PKI O = eSign Australia
Issuer (Distinguished Name)	CN = eSign Gatekeeper Root CA OU = Gatekeeper PKI O = eSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss
Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	(critical) CA: Set; Max Path Len: 0
Key Usage	(critical) CertSign and CRLSign
Certificate Policies	Certificate Policy OID: 1.2.36.88021603.333.2.3 Policy Qualifier OID: 1.3.6.1.5.5.7.2.1 https://www.esign.com.au/GKRPA/
CRL Distribution Point	URL=http://onsitecrl.esign.com.au/CA/GKRS.crl
Netscape Cert Type	OID 2.16.840.1.113730.1.1 value 03 02 01 06
Subject Alt Name	String - VeriSign assigned Value to identify CA Key Pair
Subject Key Identifier	Set (sha1 hash of Public Key)
Authority Key Identifier	Set (sha1 hash of issuer's Public Key)
Thumbprint algorithm	sha1
Thumbprint	Thumbprint value

Table 3: Certificate Profile of VeriSign Individual CA

Type	Value
Subject (Distinguished Name)	CN = eSign Grade [1, 2 or 3] Gatekeeper Individual CA OU = Terms of use at https://www.esign.com.au/GKRPA/ OU = Gatekeeper PKI O = eSign Australia
Issuer (Distinguished Name)	CN = Gatekeeper Root CA OU = Gatekeeper PKI O = eSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss
Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	(critical) CA: Set; Max Path Len: 0
Key Usage	(critical) CertSign and CRLSign
Certificate Policies	Certificate Policy OID: 1.2.36.88021603.333.2.1 Policy Qualifier OID: 1.3.6.1.5.5.7.2.1 https://www.esign.com.au/GKRPA/
CRL Distribution Point	URL=http://onsitecrl.esign.com.au/CA/GKRS.crl

Netscape Cert Type	OID 2.16.840.1.113730.1.1 value 03 02 01 06
Subject Alt Name	String - VeriSign assigned Value to identify CA pair
Subject Key Identifier	Set (sha1 hash of Public Key)
Authority Key Identifier	Set (sha1 hash of issuer's Public Key)
Thumbprint algorithm	sha1
Thumbprint	Thumbprint value

Table 4: Certificate Profile of VeriSign Non-Individual CA

Type	Value
Subject (Distinguished Name)	CN = eSign Grade [1,2 or 3] Gatekeeper Non Individual CA OU = Terms of use at https://www.esign.com.au/GKRPA/ OU = Gatekeeper PKI O = eSign Australia
Issuer (Distinguished Name)	CN = Gatekeeper Root CA OU = Gatekeeper PKI O = eSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss
Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	(critical) CA: Set; Max Path Len: 0
Key Usage	(critical) CertSign and CRLSign
Certificate Policies	Certificate Policy OID: (1.2.36.88021603.333.2.2) Policy Qualifier OID: 1.3.6.1.5.5.7.2.1 https://www.esign.com.au/GKRPA/
CRL Distribution Point	URL=http://onsitecrl.esign.com.au/CA/GKRS.crl
Netscape Cert Type	OID 2.16.840.1.113730.1.1 value 03 02 01 06
Subject Alt Name	String - VeriSign assigned Value to identify CA pair
Subject Key Identifier	Set (sha1 hash of Public Key)
Authority Key Identifier	Set (sha1 hash of issuer's Public Key)
Thumbprint algorithm	sha1
Thumbprint	Thumbprint value

Table 5: Certificate Profile of Type 3 CA (Device)

Type	Value
Subject (Distinguished Name)	CN = Gatekeeper Type 3 CA OU = Terms of use at https://www.esign.com.au/GKRPA/ OU = Gatekeeper PKI O = VeriSign Australia
Issuer (Distinguished Name)	CN = Gatekeeper Root CA OU = Gatekeeper PKI O = eSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss

Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	(critical) CA: Set; Max Path Len: 0
Key Usage	(critical) CertSign and CRLSign
Certificate Policies	Certificate Policy OID: 1.2.36.88021603.333.1 Policy Qualifier OID: 1.3.6.1.5.5.7.2.1 https://www.esign.com.au/GKRPA/
CRL Distribution Point	URL=http://onsitecrl.esign.com.au/CA/GKRS.crl
Netscape Cert Type	OID 2.16.840.1.113730.1.1 value 03 02 01 06
Subject Alt Name	String - VeriSign assigned Value to identify CA pair
Subject Key Identifier	Set (sha1 hash of Public Key)
Authority Key Identifier	Set (sha1 hash of issuer's Public Key)

Table 6: Certificate Profile of Type 3 Host CA (Device)

Type	Value
Subject (Distinguished Name)	CN = Gatekeeper Type 3 Host CA OU = Terms of use at https://www.esign.com.au/GKRPA/ OU = Gatekeeper PKI O = VeriSign Australia
Issuer (Distinguished Name)	CN = Gatekeeper Root CA OU = Gatekeeper PKI O = eSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss
Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	(critical) CA: Set; Max Path Len: 0
Key Usage	(critical) CertSign and CRLSign
CRL Distribution Point	URL=http://onsitecrl.esign.com.au/CA/GKRS.crl
Netscape Cert Type	OID 2.16.840.1.113730.1.1 value 03 02 01 06
Subject Alt Name	String - VeriSign assigned Value to identify CA pair
Subject Key Identifier	Set (sha1 hash of Public Key)
Authority Key Identifier	Set (sha1 hash of issuer's Public Key)

Table 5: Certificate Profile of Fedlink CA (Device)

Type	Value
Subject (Distinguished Name)	CN = eSign Fedlink CA OU = Gatekeeper PKI O = eSign Australia Limited
Issuer (Distinguished Name)	CN = eSign Fedlink CA OU = Gatekeeper PKI O = eSign Australia Limited
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss
Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	CA: Set; Max Path Len: 0

Key Usage	CertSign and CRLSign
Certificate Policies	Certificate Policy OID: 1.2.36.88021603.333.4.2 Policy Qualifier OID: 1.3.6.1.5.5.7.2.1 http://www.esign.com.au/RPA/Fedlink/
Netscape Cert Type	OID 2.16.840.1.113730.1.1 value 03 02 01 06
Subject Alt Name	String - VeriSign assigned Value to identify CA pair
Subject Key Identifier	Set (sha1 hash of Public Key)
Authority Key Identifier	Set (sha1 hash of issuer's Public Key)

7.1.1 Version Number(s)

The VeriSign CA supports and uses Version 3 Certificates as is indicated in the Certificate Profiles above.

7.1.2 Certificate Extensions

The VeriSign CA supports and uses Version 3 Certificate Extensions as is indicated in the Certificate Profiles above.

7.1.3 Algorithm object identifiers

The VeriSign CA supports the following algorithms approved by DSD for the use with Gatekeeper Certificates:

Algorithm	Use
md5 RSA	ABN-DSCs must use this algorithm. Preferred and default algorithm.
sha1 RSA	Optional algorithm

7.1.4 Name forms

Certificates Issued under this CPS must contain the full Distinguished Name of the CA Issuing the Certificate in the "Issuer Distinguished Name" field.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The OID for each CP that identifies the CP under which a Certificate is issued is contained in the Certificate Profile of the relevant CP.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

The VeriSign CA supports the use of syntax and semantics policy qualifiers as is indicated in the relevant Certificate Profile.

7.1.9 Processing semantics for the critical Certificate Policy extension

This policy does not require the Certificate Policies extension to be critical.

7.2 CRL Profile

CRL Field/Extension	Content
Version	V1
Signature	md5
Issuer Distinguished Name	CA Distinguishing Name that issued the CRL.
ThisUpdate	The time this revocation list was issued.
NextUpdate	The time the next revocation list will be issued.
RevokedCertificates	Serial Numbers of the Certificates that have been revoked.
AuthorityKeyIdentifier	Identifies the CA Public Key to be used to verify the signature of the Certificate.
InvalidityDate	The time at which it is known or suspected that the Private Key was

	Compromised (this may be earlier than the date the Certificate was Revoked).

1. The location of the CRL for a Certificate is published in the Certificate Extension field of the Certificate named "CRL Distribution Point".

2. The location of the OCSP responder for a Certificate is published in the Certificate Extension field of the Certificate named "CRL Distribution Point".

7.2.1 Version number(s)

1. The VeriSign CA supports and uses X.509 Version 1 CRLs.

2. The VeriSign CA operates an OCSP responder for most CAs, and applications that interface with the OCSP responder can check the status of Certificates in real time without needing to consult the CRL for those CAs.

7.2.2 CRL and CRL entry extensions

The VeriSign CA supports and uses X.509 Version 1 CRL entry extensions as is indicated in the CRL profile above.

8 SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

1. The following process describes how changes to an Approved Document may be affected:

   (a) 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 VeriSign CAs and/or RAs;

   (b) the change is submitted to the Policy Approval Authority, which reviews the change request, assesses whether the change request is required, and if it deems it necessary, returns the change request with comments suggesting any further work required before the request is submitted to Finance;

   (c) on determining that the change request is suitable for submission to Finance, and that the changes required are clearly explained and documented, the Policy Approval Authority will forward a copy of the requested changes to Finance along with any supporting documentation that the Policy Approval Authority deems appropriate for the proper consideration of the change request;

   (d) the Policy Approval Authority is responsible for liaising with Finance and, if deemed appropriate by the Policy Approval Authority, the change request sponsor, to ensure the timely consideration of the change request;

   (e) a change can only be made to the Approved Documents once approval has been granted by the Competent Authority; and

   (f) the VeriSign CA 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.

2. 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 Policy Approval Authority.

3. If a change is made to this Certificate Policy that materially affects the assurance provided, then it may be necessary for the VeriSign CA to modify the Certificate Policy Object Identifier. If this occurs, the VeriSign CA will contact affected Subscribers.

8.2 Publication and notification policies

1. The VeriSign CA will maintain all publicly accessible Approved Documents in the Repository. Changes to all publicly accessible Approved Documents will also be published in the Repository.

2. The VeriSign CA will inform any of its PKI Service Providers of all changes to Approved Documents directly, and will use reasonable endeavours to do this.

8.3 CPS approval procedures

The Competent Authority is responsible for approving changes to this CPS.