VERISIGN
TYPE 3 CERTIFICATE POLICY
(VERISIGN GATEKEEPER TYPE 3 CP)

Date of Publication: July 2004
Proposed Effective Date: July 2004

TABLE OF CONTENTS

1. INTRODUCTION

1.0 Structure of this Certificate Policy and relationship to CPS*

1. VeriSign Australia Pty Ltd trading as eSign Gatekeeper Services ('**eSign**') provides both Public and Private certification services using technology from VeriSign Inc. This Certificate Policy ("**CP**") sets out a number of policy and operational matters in relation to the Gatekeeper Type 3 Certificate ("**Device Certificate**").

2. This CP covers only those matters specific to the Type 3 Certificate including the obligations of the PKI Entities. For more information about VeriSign's functions as a CA you should read the VeriSign Gatekeeper CPS. The obligations of the PKI Entities are also set out in the relevant Subscriber Agreement and Relying Party Agreement.

3. The headings of this CP 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 CP (e.g. this section). These are indicated by an asterisk (*) after the heading.

4. The provisions of this CP in relation to Type 3 Certificates prevail over the provisions of the VeriSign Gatekeeper CPS to the extent of any direct inconsistency.

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

1.1 Overview

1. The Type 3 Certificate is used to identify an application, Device, process or service that is owned, operated or controlled by an Organisation. For example a Type 3 Certificate may be installed on a Device to enable an Organisation to:

   (a) automatically digitally sign communications from an Organisation (eg an email auto-responder, an email generated by a software process, or an electronic data interchange (**EDI**) software client); or

   (b) automatically encrypt communications sent to an Organisation (eg when email is sent to a generic drop box (eg support@organisation.com.au) or to an EDI server/client).

2. One Certificate is able to be Issued under this Certificate Policy that can be used for Signing and Encryption.

3. To obtain a Type 3 Certificate an Organisation must first obtain an ABN-DSC and have a current Authorised Officer. The Authorised Officer must be authorised to act on behalf of the Organisation in relation to Type 3 Certificates. During the process for applying for ABN-DSCs processes are performed to identify the Organisation and the Authorised Officer. See further the VeriSign ABN-DSC CP.

1.2 Identification

This CP is known as the "VeriSign Gatekeeper Type 3 CP". The OID for this is 1.2.36.88021603.333.2.8. Some certificates issued between 24 April 2003 and 1st July 2004 will contain the OID 1.2.36.2038371.333.2.8.

1.3 Community and applicability

The community of interest for this CP comprises Organisations who wish to transact with others including Government.

1.3.1 Certification Authorities (CAs)

1. The Certification Authority (CA) that Issues Type 3 Certificates under this CP is the VeriSign CA, operated by VeriSign Australia Pty Ltd or a Subordinate CA. The functions and obligations of a Subordinate CA are the same as those of the VeriSign CA under this CP and the CPS.

2. This CP does not apply to Certificates Issued by the VeriSign CA to Subordinate CAs, or any other type of Certificate apart from Type 3 Certificates.

1.3.2 Registration Authorities (RAs)

1. The VeriSign RA or another Gatekeeper Accredited RA will perform the functions of the Registration Authority.

2. Where an RA function under this CP is performed by a person other than the VeriSign RA, that RA will be bound contractually by VeriSign to perform the Registration functions in accordance with the CP and other Approved Documents.

1.3.3 End Entities

The End Entities to which this CP applies are Subscribers and Relying Parties.

1.3.4 Applicability

1.3.4.1 Scope of use of Type 3 Certificates*

The purpose of Certificates and Key Pairs Issued under this CP is to facilitate electronic transactions with, and on behalf of, Agencies and others, and more particularly to enable a Subscriber to install a Certificate on a Device to enable a Device to:

(a) authenticate itself to a Relying Party electronically in online transactions;

(b) digitally sign electronic documents, transactions and communications; and

(c) confidentially communicate with a Relying Party.

1.3.4.2 Restrictions on use*

1. NOIE has recommended the following restrictions on the use of Type 3 Certificates:

Certificate	Restriction	
	Sensitive Information	**Financial Implications**
Type 3	Up to and including Protected information.	Any limitation to be determined by transacting parties.

2. VeriSign has specifically limited its liability in respect of Gatekeeper Certificates as specified in section 2.2 of this CP.

3. VeriSign's services under this CP and the CPS are not designed, intended, or authorised for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

*1.3.5 Gatekeeper Accreditation**

The VeriSign RA has been granted Gatekeeper Accreditation to Verify the identity of Subscribers, and the VeriSign CA to Issue Type 3 Certificates under this CP, and perform the other functions specified in this CP, in accordance with this CP.

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 CP 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:	Manager, Gatekeeper National Office for the Information Economy
Physical Address	28 National Circuit, Forrest ACT
Postal Address	National Office for the Information Economy GPO Box 390, Canberra ACT 2601
Email	webmaster@noie.com.au
Facsimile	+61 2 6271 1616

1.4.5 Person determining CPS suitability for this CP

The Competent Authority has determined that the VeriSign Gatekeeper CPS is suitable for this 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 CP and the 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 CP or upon prior written approval from VeriSign.
3. This CP serves as notice of the rules governing the respective rights and obligations of the PKI Entities among themselves.
4. The VeriSign RA and VeriSign CA is deemed to have agreed to the CP on its publication by VeriSign.
5. Where an entity wishes to obtain Keys and Certificates under this CP, that entity is deemed to be bound by the provisions of this CP applicable to:
   (a) the Authorised Officer – when it approves the Issuance of a Certificate; and
   (b) the Organisation – when it signs the Subscriber Agreement.
6. An entity is deemed to be bound by the provisions of this CP applicable to a Relying Party when the entity relies on a Certificate Issued under this CP.

*2.1.0 RCA Obligations**

1. The root Certification Authority for the purposes of this CP is the VeriSign Gatekeeper Root (VGR).
2. The VGR signs the certificate of the VeriSign CA.

3. The functions and obligations of the VGR are set out in the CPS.

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 the Subscriber, that:

(a) the Relevant RA has confirmed that Verification has been successfully completed in accordance with **section 3.1.8A – 3.1.10**;

(b) the Certificate Information provided by the Relevant RA (or the Authorised Officer) has been accurately transcribed into the Certificate;

(c) all material information contained in the Certificate (other than that specified in **paragraph (b))** is accurate; and

(d) the Certificate contains all the elements required by the Certificate Profile.

2.1.1.2 Key Management*

1. The VeriSign CA neither generates nor holds the Private Keys of Subscribers.

2. The VeriSign CA cannot ascertain or enforce any particular Private Key protection requirements on 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**;

(b) promptly Revoke a Certificate if requested by the Subscriber or as otherwise required under **section 4.4**; and

(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;

(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

The Relevant RA must:

(a) properly conduct the Verification process described in **sections 3.1.8A – 3.1.10**;

(b) ensure the accuracy and completeness of any part of the Certificate Information which is generated or compiled by the Relevant RA;

(c) ensure that all relevant information concerning a Certificate is recorded (electronically or otherwise) for an appropriate period of time (in the case of Certificates being Issued to an Agency, as specified

in policies and guidelines issued by the National Archives of Australia under the *Archives Act 1983* (Cth)), and in particular, for the purpose of providing evidence for the purposes of legal proceedings;

(d) utilise Trustworthy Systems, procedures and human resources in performing its services; and

(e) comply with any other relevant provisions of this CP (in particular, **section 2.8**) and the Approved Documents.

*2.1.3 Subscriber Obligations**

THE ORGANISATION ACKNOWLEDGES THAT IT, AND NOT VERISIGN, IS EXCLUSIVELY RESPONSIBLE FOR PROTECTING ITS PRIVATE KEY(S) FROM COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORIZED USE.

1. The obligations of a Subscriber are imposed on the Organisation and the Authorised Officer who acts on behalf of the Organisation as set out in this **Section 2.1.3**.

2. Organisations must through an Authorised Officer:

   (a) ensure that only appropriately authorised people perform any of the functions specified in **section 3.1.11.2**;

   (b) ensure that Private Key(s) are generated using a Trustworthy System;

   (c) ensure that anyone performing any of the functions specified in **section 3.1.11.2** comply with their obligations under this CP and the CPS;

   (d) provide measures to avoid Compromise. loss, disclosure, modification or unauthorised use of Private Keys;

   (e) immediately notify the VeriSign CA when the Organisation becomes aware that a Private Key has been Compromised, or there is a substantial risk of Compromise;

   (f) ensure that all information provided to the VeriSign CA or the Relevant RA in relation to Issue and use of their Key Pairs and Certificates is to the best of their knowledge, true and complete;

   (g) immediately notify the VeriSign CA or the Relevant RA if:

      (i) there is any other change to the Registration Information, or any other information provided to the Relevant RA in relation to Issuance and use of their Certificates.

      (ii) the Device on which the Certificate is installed is sold, decommissioned, destroyed or lost;

      (iii) the application, Device, process or service identified by the Certificate ceases to be under the control of the Organisation; or

      (iv) the Organisation ceases to belong to the Community of Interest;

   (h) if requested by the Relevant RA, provide complete and accurate Registration Information or anything else relating to Issuance or use of the Keys and Certificates;

   (i) use Keys and Certificates only for the purposes which they were Issued and within the usage and reliance limitations, as specified in this CP, the Certificate Profile and the Certificate;

   (j) check the details set out in a Certificate on receipt, and promptly notify the VeriSign CA if faulty or improper Registration or Certificate Issuance has occurred; and

   (k) where they generate Key Pairs, comply with **section 6.**

3. The Organisation agrees not to copy the Certificate (except for the purposes of backup and Escrow as permitted under this Certificate Policy) or to use the Certificate on more than one Device.

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 Expired or been Revoked 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 CPS or this CP.

2. If a Relying Party relies on a Digital Signature or Certificate in circumstances where it has not been Validated in accordance with **paragraph 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 CP 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 Device 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 Subscriber 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 CPS or this CP by the Subscriber;

   (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 CP.

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 FROM VERISIGN OF ANY RIGHTS OR PRIVILEGES, EXCEPT AS SPECIFICALLY PROVIDED IN THE CPS OR THIS CP.

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

4. 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 CP.

2.2 Liability[1]

*2.2.1 Liability Generally**

1. The liability of an entity referred to in this CP 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 CP by the VeriSign CA or the VeriSign RA is not evaluated by NOIE Authorised Legal Evaluators or 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:

   (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 Accredited Documents;

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

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

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

*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 CPS or this CP 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 CP. 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 and Relevant RA 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 CP; 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 including 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 CPS or this CP, breach of contract or any express or implied warranty or indemnity under or in relation to any Certificates or the CPS or this CP 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 AUD50,000.

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**

2.2.5.1 Organisation

1. The Organisation is responsible and therefore liable for any acts of Authorised Officers or those to whom obligations have been delegated in relation to the CPS and this CP, and in particular in relation to the use of Keys and Certificates Issued under this CP.

2. The Organisation:

   (a) is solely responsible for the contents of any transmission, message or other document signed using the Private Key of the Certificate;

   (b) warrants to all Relying Parties that during the Operational Period of the Certificate, and until notified otherwise by the Organisation that:

      (i) no unauthorised person has ever had access to the Certificate's Private Key;

      (ii) the Certificate will be used exclusively for appropriate and lawful purposes;

(iii) at the time the Digital Signature is created, the Certificate has not Expired or been Suspended or Revoked;

(iv) all representations made by the Organisation, or authorised by the Organisation or the Authorised Officer to the VeriSign CA or to the Relevant RA, are true;

(v) all information contained in the Certificate is to the Organisation's and the Authorised Officer's knowledge true and complete;

(vi) each Digital Signature created using the Private Key Corresponding to the Public Key listed in the Certificate is the Organisation's Digital Signature;

(vii) the Organisation will not allow the Private Key Corresponding to any Public Key listed in the Certificate to be used for purposes of signing any Digital Certificate (or any other format of certified Public Key) or Certificate Revocation List, unless expressly agreed in writing with VeriSign, and

(viii) when the Organisation encrypts the hash of a document with the Private Key, in circumstances where the Certificate has not been Suspended or Revoked, others may act on that as if the Organisation had signed the document with the Organisation's usual signature in the normal way;

(c) indemnifies the VeriSign CA and the Relevant RA for any loss, damage and expense of any kind, arising out of or in connection with:

(i) the Organisation's or the Authorised Officer's negligence or wilful misconduct;

(ii) any falsehood or misrepresentation of fact by the Organisation or the Authorised Officer (or any person acting on the Organisation's instructions);

(iii) the Organisation's or the Authorised Officer's failure to disclose a material fact, if the misrepresentation or omission was made negligently or with the intent to deceive the VeriSign CA or the Relevant RA or any person receiving or relying on the Certificate; or

(iv) any failure by the Organisation or the Authorised Officer to protect the Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the Compromise, loss, disclosure, modification, or unauthorised use of the Private Key,

except to the extent that the Subscriber's Private Key or Certificate has been Compromised by VeriSign's or the Relevant RA's wilfully wrongful, fraudulent or negligent conduct.

(d) indemnifies the VeriSign CA and the Relevant RA for any loss, damage and expense of any kind, arising out of or in connection with the manner and extent of the use or publication of the Organisation's Certificate except to the extent that:

(i) the use or publication of that Certificate was caused by the VeriSign CA or the Relevant RA using or publishing the Certificate other than as allowed by this CP; or

(ii) the Organisation's Private Key or Certificate has been Compromised by VeriSign's or the Relevant RA's wilfully wrongful, fraudulent or negligent conduct.

2.2.5.2 Key Holder Liability

No stipulation.

2.2.5.3 Authorised Officer Liability

Organisations are responsible and liable for the use made by Authorised Officers of Certificates and Keys and the instructions issued to the VeriSign CA and PKI Entities by the Authorised Officer. Organisations may make their own arrangements with Authorised Officers concerning the policies and procedures for use of the Certificates and Keys and providing Issuing and Revocation instructions to the VeriSign RA and PKI Entities, and liability provisions.

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 this CP, the 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. This CP and the 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 this CP or the 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 CP 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) this CP;

(b) the CPS;

(c) the Type 3 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 Entities 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

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 VeriSign 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 the VeriSign CA previously Issued a certificate erroneously.

2.6 Publication and 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) this CP;

(e) the 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. See further **section 4.4.10**.

2.6.3 Access controls

1. There are no controls on read-only access to this CP, the 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

The VeriSign CA is required to conduct periodic audits of its operations and is also subject to external audits by the Competent Authority. Details are set out in **section 2.7** of the CPS.

2.8 Privacy and Data Protection

2.8.1 Types of information to be kept confidential

2.8.1.1 Confidential Information*

Each PKI Entity must protect Confidential Information it holds against unauthorised disclosure.

2.8.1.2 Personal Information*

1. The Registration Information may contain Personal Information about individuals.

2. The Relevant RA must not collect any Personal Information about individuals as part of the Registration process other than the Registration Information and other necessary information to complete the transaction.

3. The VeriSign CA and the Relevant RA must comply with their obligations under the *Privacy Act 1988 (Cth)*, including (where applicable) the National Privacy Principles or any approved privacy code.

4. When providing services to or in relation to a Commonwealth Agency, the VeriSign CA and the Relevant RA must also comply with the Information Privacy Principles, as if they were Agencies of the Commonwealth of Australia.

5. When providing services to or in relation to a State or Territory Agency, the VeriSign CA and the Relevant RA must also comply with:

   (a) any privacy law applicable to service providers to that agency; and

   (b) any other privacy obligations imposed by or in relation to that agency.

2.8.1.3 Other information which is protected*

Certain information provided to a PKI Service Provider will be protected under specific legislation, or guidelines. The PKI Service Provider agrees to protect that information in accordance with the applicable legislation or guidelines, or in accordance with any procedures agreed between the PKI Service Provider and an Agency.

2.8.2 Types of information not considered confidential

2.8.2.1 Certificate Information*

Subscribers agree to the publication, through the Certificate Directory and CRL, of any Personal Information which forms part of the Certificate Information.

2.8.3 Disclosure of Certificate Revocation/Suspension information

Revocation of a Certificate will be published in the CRL in accordance with this CP.

2.8.4 Release to law enforcement officials

Personal Information, Confidential Information and other information which is protected under **section 2.8.1.3** must not be released by a PKI Service Provider to law enforcement agencies or officials except under a properly constituted warrant or unless otherwise legally required.

2.8.5 Release as part of civil discovery

Personal Information, Confidential Information and other information which is protected under **section 2.8.1.3** must not be released by a PKI Service Provider except under a properly constituted order from a court or other body having power to require production of that information, or unless otherwise legally required or authorised.

2.8.6 Disclosure upon owner's request

1. The subject of any Personal Information held by a PKI Service Provider shall on request be provided with that information in accordance with the PKI Service Provider's Personal Information access protocol, and the privacy obligations applicable to the PKI Service Provider under this CP, and if there is any inconsistency between the two, in accordance with those privacy obligations.
2. Subject to any applicable law or legal restriction, Personal Information held by a PKI Entity about a Subscriber may be disclosed to a third party where the Subscriber has authorised the disclosure in writing.

2.8.7 Other information release circumstances

No stipulation.

2.9 Intellectual Property Rights

1. Unless otherwise agreed between the relevant PKI Entities:
   (a) Intellectual Property Rights (IP Rights) in the Approved Documents, the Certificate Directory and the CRL are owned by VeriSign;
   (b) IP Rights in Certificates are owned by VeriSign, subject to any pre-existing IP rights which may exist in the Certificates or the Certificate Information; and
   (c) any IP rights in Key Pairs are owned by the PKI Entity which generated the Key Pair.
2. The PKI Entity which owns IP Rights in Certificates, Distinguished Names and Key Pairs grants to any other relevant PKI Entity which has a requirement under this CP, the CPS or the Approved Documents to use that Intellectual Property, the rights it reasonably requires to perform that entity's roles, functions and obligations under this CP, the CPS or the Approved Documents.
3. The PKI Entity that owns the relevant IP Rights warrants that:
   (a) it has the rights necessary to grant the licences described in **section 2.9.2;** and;
   (b) the use by PKI Entities of the relevant IP pursuant to this CP, the CPS or other Approved Documents will not infringe the IP Rights of a third party.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

1. The VeriSign CA will assign a Distinguished Name to each Type 3 Certificate Issued based on the Registration Information.

2. The VeriSign CA may refuse to assign a Distinguished Name based on the Registration Information on reasonable grounds - for example where the Distinguished Name is likely to:

   (a) be obscene or offensive;

   (b) mislead or deceive Relying Parties (including where the pseudonym has already been issued to an individual);

   (c) infringe the IP Rights of any person; or

   (d) otherwise be contrary to law.

3. The Distinguished Name to be included in the "Subject" field of a Type 3 Certificate shall be constructed in accordance with the table below:

Standard Attribute Type	Value	Example
Common Name	Application or Device Name	CN = CCF Email Gateway
User Defined (optional)	Any user defined data	OU = CCF 1
User Defined (optional)	Any user defined data eg Trading Name	OU = Acme Imports
Organisation	Legal Entity Name	O = Acme Pty Ltd
State or Province	State	S = NSW
Country	Australia	C = AU

3.1.2 Need for names to be meaningful

1. Distinguished Names that are created based on information provided in the application are assumed to be meaningful.

2. Anonymous Certificates are not supported.

3.1.3 Rules for interpreting various name forms

Distinguished Names must include each of the elements specified in the relevant X.509 – compliant Certificate Profile.

3.1.4 Uniqueness of names

The Subject (Distinguished Name) allocated by the VeriSign CA will be unique. This is enforced through software operated by the VeriSign CA.

3.1.5 Name claim dispute resolution procedure

Disputes regarding assignment of Distinguished Names must be resolved under **section 2.4.3**.

3.1.6 Recognition, authentication and role of trademarks

1. Trade mark rights or other IP Rights may exist in the Organisation's name, or other parts of the Registration Information or Certificate Information.

2. By applying for Registration, the Subscriber, and the Organisation:

   (a) authorise the VeriSign CA and other PKI Service Providers to use the relevant Intellectual Property for the purpose of creating a Distinguished Name and for other purposes reasonably necessary in relation to Issuance of Keys and Certificates to, and their use by, the Organisation and its Subscribers;

(b) warrant that they are entitled to use that Intellectual Property for the purposes for which Keys and Certificates are Issued and may be used, without infringing the rights of any other person; and

(c) agree to indemnify the VeriSign CA other PKI Service Providers, and their respective officers, employees, contractors and agents against loss, damage, costs or expenses of any kind (including legal costs on a solicitor-client basis) incurred by them in relation to any claim, suit or demand in respect of an infringement or alleged infringement of the IP Rights of any person.

3. The VeriSign CA does not independently check the status of any trademark or other IP Rights.

3.1.7 Method to prove possession of Private Key

The VeriSign CA verifies that the Private Key is installed on the Device's through the use of a digitally signed certificate request pursuant to PKCS #10, another Cryptographically-equivalent demonstration, or another VeriSign CA-approved method.

*3.1.8A Verification**

1. The Relevant RA must perform the relevant checks before a Certificate is Issued.

2. These checks involve confirming that:

(a) an Authorised Officer is authorised to request Certificates on behalf of the Organisation;

(b) the Authorised Officer has authorised the Issuance of a Certificate with the Subject (Distinguished Name) entered into the VeriSign system; and

(c) the Authorised Officer authorising the Issuance of the Certificate has an ABN-DSC with the same ABN and Organisation name as that which is requested to appear in the Certificate.

3. No checking is performed by the VeriSign CA or VeriSign RA that:

(a) the Subject (Distinguished Name) is meaningful; or

(b) that the Certificate is being used in the manner indicated by the Subject (Distinguished Name) (ie VeriSign can not confirm that a Certificate purportedly identifying a particular Device operated by the Organisation is in fact installed on that Device).

4. As an Organisation must have first obtained an ABN-DSC, it can be assumed for the purpose of this CP that the Organisation has been Verified and also that the identity of the Authorised Officer has been Verified.

5. The Device or application that is to be Issued with a Certificate is not Verified by the VeriSign RA. A digitally signed email or other notice from an Authorised Officer, requesting Issue of a Type 3 Certificate will be accepted by the VeriSign CA as sufficient proof that the Organisation requires a Certificate with the corresponding Private Key to be Issued on behalf of the Organisation.

3.1.8 Verification of identity of Organisation

None. As an Organisation must have first obtained an ABN-DSC, it can be assumed for the purpose of this CP that the Organisation has been Verified.

3.1.9 Verification of Identity of an Individual

None.

3.1.9.1 Verification of Identity of the Authorised Officer

The VeriSign RA must confirm that the person authorising the Issuance of a Certificate is a current Authorised Officer of the Organisation.

3.1.9.2 Verification of Identity of an Applicant

No Verification is performed on the person who enters the details to appear in a Certificate.

3.1.10 Verification of the Authority of a Key Holder

No stipulation.

3.1.11 Authorised Officer

A Business Entity which intends to authorise the use of Type 3 Certificates must have at least one Authorised Officer.

3.1.11.1 *Not Used.*

3.1.11.2 Functions of Authorised Officer*

1. The functions of the Authorised Officer under this CP include:

   (a) identifying and locating Devices upon which Certificates are installed;

   (b) requesting Type 3 Certificates be Issued by the VeriSign CA;

   (c) accepting Type 3 Certificates on behalf of the Organisation;

   (d) ensuring that Type 3 Certificates are installed on the appropriately identified Devices; and

   (e) managing Type 3 Certificates on Devices within the Organisation; and

   (f) requesting Type 3 Certificates be Revoked.

2. The Authorised Officer may delegate these functions (except that mentioned in **paragraph (b)**) to a person or organisation acting on behalf of the Organisation. Delegation does not relieve the Authorised Officer of responsibility for ensuring these tasks are performed. A person or organisation to whom these functions are delegated must fulfil those functions in accordance with this CP.

3.2 Routine ReKey (Renewal)

Device Certificates may not be renewed however a new Certificate can be applied for with the same Distinguished Name as the old Certificate.

3.3 Reissue

1. Provided that it is proved to the VeriSign CA's satisfaction that an Organisation has had a technical problem with its Certificate (such as a problem in installing the Certificate), and a new Certificate is required to be Issued, the VeriSign CA may, at its discretion, provide a new Certificate.

2. Subscribers applying for the Issue of a new Certificate after Revocation must undergo the following procedure:

   (a) Apply for a new Certificate online; and

   (b) Have the Authorised Officer approve the Issuance of the Certificate and communicate this fact to the VeriSign RA by means of a digitally signed email.

3.4 Revocation Request

1. Before processing a request for Revocation of a Certificate, the VeriSign CA must Verify that the request is made by a person or entity authorised to request Revocation of that Certificate under **section 4.4.2**.

2. A request for Revocation can be Verified in the following ways:

   (a) the request is digitally signed with the Private Key of an Authorised Officer; or

   (b) the request is made in person, and the authority of the requestor is Verified as required under **section 3.1.10** of the ABN-DSC CP; or

   (c) the request is made using a Challenge Phrase provided at the time of Registration.

3. The VeriSign CA's detailed procedures for Verifying Revocation requests is set out in the CA Operations Manual.

4. OPERATIONAL REQUIREMENTS

4.0 Operations Manuals*

1. The VeriSign CA maintains a CA Operations Manual that details the operational practices of the VeriSign CA in relation to its functions and obligations under this CP.

2. The VeriSign RA maintains a RA Operations Manual that details the operational practices of the VeriSign RA in relation to its functions and obligations under this CP.

4.1 Certificate Application

*4.1.1 Registration**

1. The VeriSign RA provides an online enrolment process for the Issuance of Certificates. See the VeriSign Gatekeeper Website for further information and a step by step guide for enrolling for a Certificate.
2. An Organisation, which is within the Community of Interest, may apply to the VeriSign RA for a Type 3 Certificate to be Issued to the Organisation.
3. An Organisation can only have one Type 3 Signing and Encryption Certificate with the same Distinguished Name.

*4.1.2 Duties of PKI Service Providers**

PKI Service Providers are not required to investigate or ascertain the authenticity of any document received by them as evidence of any matter required as part of the Registration process unless they are aware, or should reasonably be aware, that the document is not authentic.

4.2 Certificate Issuance

1. Upon receiving a request for the Issuance of a Certificate, the VeriSign CA will either:
   (a) Issue a Certificate; or
   (b) refuse to Issue a Certificate.
2. The VeriSign CA is not bound to Issue a Type 3 Certificate despite receipt of an Application.
3. The VeriSign CA may refuse to Issue a Certificate, at its sole discretion, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. On the VeriSign CA's refusal to Issue a Certificate, the VeriSign CA shall promptly refund to the Organisation any paid Certificate enrolment fee less any Relevant RA processing costs and VeriSign processing costs, unless the Certificate Application contained fraudulent or falsified information. The VeriSign CA shall provide an explanation to all Organisations whose Applications have been unsuccessful.

4.3 Certificate Acceptance

1. An Organisation is deemed to have accepted a Certificate when approval is manifested by the PIN for that Certificate being entered at a URL that is emailed to the email address provided in the Registration Information.
2. The Subscriber must notify the VeriSign CA 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.
3. A Subscriber 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.
4. Once a Certificate is Issued, the VeriSign CA shall have no continuing duty to monitor or investigate the accuracy of the information in a Certificate, unless the VeriSign CA is notified in accordance with this CP of that Certificate's Compromise.
5. Certificates will be published after Issue as required by **section 2.6.2**.

4.4 Certificate Suspension and Revocation

On Revocation of a Certificate:

(a) the Certificate's Operational Period expires;
(b) the underlying contractual obligations between the Subscriber and other PKI Entities are unaffected;
(c) the Subscriber must continue to safeguard their Private Keys unless they destroy their Private Keys;
(d) the Subscriber must cease using the Certificate for any purpose whatsoever;
(e) the VeriSign CA must promptly notify the Subscriber that its Certificate has been Revoked; and

(f) the VeriSign CA must update the CRL.

4.4.1 Circumstances for Revocation

1. The VeriSign CA shall Revoke a Certificate (whether or not it has received a request to do so) where it becomes aware (or reasonably suspects) that:

   (a) there has been a loss, theft, modification, or other Compromise of the associated Private Key;

   (b) faulty or improper Registration, Key Generation or Issue of a Certificate has occurred;

   (c) a change in the Registration Information occurs;

   (d) the Certificate's associated Private Key or other Trustworthy System was Compromised in a manner materially affecting the Certificate's reliability;

   (e) the applicable Subscriber has not complied with an obligation under the CPS, this CP or the Subscriber Agreement; or

   (f) another person's information has been or may be materially threatened or Compromised unless the Certificate is Revoked.

2. The VeriSign CA shall also Revoke a Certificate:

   (a) on request by a person specified in **section 4.4.2**; or

   (b) if it becomes aware that the Subscriber has ceased to belong to the Community of Interest;

3. A PKI Service Provider is not required to investigate any of the circumstances described in **section 4.4.1**, but where those providers do decide to investigate those circumstances, they must use reasonable endeavours to notify the relevant Subscriber beforehand of that intention.

4.4.2 Who can request Revocation

1. An Organisation through an Authorised Officer or otherwise, may request the VeriSign CA to Revoke its Subscribers Certificate(s) at any time.

2. The VeriSign CA may require such proof as it deems reasonably necessary to confirm the identity of the individual requesting Revocation of a Certificate, and if it is not the Authorised Officer, its relationship with the Subscriber.

3. 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 VeriSign CA is satisfied that the entity:

   (a) is lawfully empowered to require Revocation of the Certificate; or

   (b) is lawfully entitled to administer the Organisation's affairs which relate to the Certificate(s).

4. A PKI Entity must immediately notify the VeriSign CA if:

   (a) it receives a request for Revocation of a Certificate(s); or

   (b) it becomes aware of circumstances which may justify Revocation of a Certificate(s), such as those set out in **section 4.4.1**.

4.4.3 Procedure for Revocation request

1. A Revocation request, other than one that is made in person, must be sent to the VeriSign CA by any of the methods described in **section 2.4.2.3**.

2. A Revocation request, which is made in person, must be made to the VeriSign CA at their address set out on the VeriSign Gatekeeper Website**.**

4.4.4 Revocation request grace period

There is no grace period.

4.4.5 Certificate Suspension

Certificate Suspension is not currently supported for Certificates but may be offered if there is market demand.

4.4.6 *Who can request Suspension*

See **section 4.4.5**.

4.4.7 *Procedure for Suspension request*

See **section 4.4.5**.

4.4.8 *Limits on Suspension period*

See **section 4.4.5**.

4.4.9 *CRL issuance frequency (if applicable)*

1. The VeriSign CA will update the CRL at least daily.

2. CRLs shall also be issued on an emergency basis, as determined by the VeriSign CA.

4.4.10 *CRL checking requirements*

See **sections 2.1.4-2.1.4.1**.

4.4.11 *On-line revocation/status checking availability*

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.

4.4.12 *On-line Revocation checking requirements*

To use an OCSP responder that is provided by the VeriSign CA, a person, device or application must be using appropriate software to interrogate and interpret the information provided by the OCSP responder.

4.4.13 *Other forms of Revocation advertisements available*

No stipulation.

4.4.14 *Checking requirements for other forms of Revocation advertisements*

No stipulation.

4.4.15 *Special requirements re Key Compromise*

The VeriSign CA shall use reasonable efforts to notify potential Relying Parties if the VeriSign CA discovers, or has reason to believe, that there has been Compromise of the Private Key of a VeriSign CA.

4.4A Certificate Expiry*

1. The VeriSign CA will make a reasonable effort to notify Subscribers via email at the address they provided in the Application, of the impending Expiration of their Certificates.

2. Expiration of a Certificate does not affect the Validity of any underlying contractual obligations created under the CPS or this CP.

4.5 Security Audit Procedures

The VeriSign CA is required to log particular information. Details are set out in **section 4.5** of the CPS.

4.6 Records Archival

The VeriSign CA is required to archive particular information. Details are set out in **section 4.6** of the CPS.

4.7 Key changeover

1. Two years before the Expiry of the VeriSign CA or a Subordinate CA's Certificate, the VGR will re-certify the CA's Certificate, giving it a further 10 year Operational Period.

2. In the case of the VGR, the VGR will re-certify its own Certificate.

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 CP 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 the Certificate of the VeriSign CA or a Subordinate 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 the Private Key of the VeriSign CA or a Subordinate CA 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 CP; 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 CP 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 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

1. **Section 5** of the CPS sets out the practices and procedures of the VeriSign CA in respect of the following topics:

(a) General*

(i) Security Policy*

(ii) Protective Security Risk Review*

(iii) Protective Security Plan*

(b) Physical Controls

(i) Site location and construction

(ii) Physical access

(iii) Power and air conditioning

(iv) Water exposures

(v) Fire prevention and protection

(vi) Media storage

(vii) Waste disposal

(viii) Off-site backup

(c) Procedural Controls

(i) Trusted roles

(ii) Number of persons required per task

(iii) Identification and authentication for each role

(d) Personnel Controls

(i) Background, qualifications, experience, and clearance requirements

(ii) Background check procedures

(iii) Training requirements

(iv) Retraining frequency and requirements

(v) Job rotation frequency and sequence

(vi) Sanctions for unauthorised actions

(vii) Contracting personnel requirements

(viii) Documentation supplied to personnel

By reading the CPS, a PKI Entity can gain an appreciation of the measures taken by VeriSign to ensure that the VeriSign CA and VeriSign RA are able to provide their services in a secure, reliable and trusted manner.

6. TECHNICAL SECURITY CONTROLS

6.0 Key Management*

1. This section deals with the generation and distribution of Keys for Subscribers only. For information regarding the VeriSign CA's generation and distribution of its CA Keys see this section in the CPS.

2. Subscribers should instigate their own policies to ensure the integrity, and security of the Type 3 Certificate Private Keys. The VeriSign CA recommends the backup of Type 3 Certificates.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair generation

1. Key Pair generation must 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. A Certificate's Key Pair(s) are generated and stored by the application that generates those Keys (eg a browser) during the Application process.

6.1.2 Private Key delivery to Entity

1. As the Private Keys are generated and stored by the Device (eg a browser or Hardware Security Module device) used by the Organisation, there is no need for the VeriSign CA or the VeriSign RA to see or deliver any Private Keys to Subscribers.

2. The Organisation may be required to export the Key Pair and associated Certificate, from the browser where the Key Pair was generated, and import it into the required Device to identify the relevant application, Device, process or service for which it was Issued.

6.1.3 Public Key Delivery to Certificate Issuer

1. A Certificate's Public Key is forwarded to the VeriSign CA as part of the Key Generation process. When a Public Key is transferred to the VeriSign 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 Organisation possesses the Private Key corresponding to the transferred Public Key such as using a PKCS#10 message or other cryptographically-equivalent method.

2. Upon the Acceptance of the Certificate, the VeriSign CA shall publish a copy of the Certificate in the Certificate Directory and in other appropriate locations, as determined by the VeriSign CA. Subscribers may publish their Certificates in locations of their choosing.

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 Organisation as part of the process of Issuance of a Certificate to an Organisation, 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 for download in the Repository.

6.1.5 Key sizes

The VeriSign CA's online Application process checks the Key size of Keys and ensures that all Keys generated by the Organisation are 1024 bits or longer.

6.1.6 Public Key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 *Hardware/software Key generation*

Key Pairs are generated by Organisations using algorithms embedded in the application/hardware used to generate the Keys. These algorithms should be of the strength and type specified in Annex H of the Gatekeeper Report (basically products listed on the Evaluated Products List).

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. For key usage regarding this CP, see the Certificate Profile at **section 7** of this CP.

6.2. Private Key Protection

Private Keys shall be protected by Subscribers and Organisations using a Trustworthy System and Subscribers shall take necessary precautions to prevent the loss, disclosure, modification or unauthorised use of such Private Keys.

6.2.1 *Standards for Cryptographic Module*

The Subscriber should ensure that the Cryptographic Module used to store its Private Key adequately protects its Private Key from Compromise.

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

No stipulation.

6.2.3 *Private Key Escrow*

Subscribers should not Escrow their Private Keys.

6.2.4 *Private Key backup*

Subscribers may make their own arrangement for backup of their Private Keys used for decryption. Subscribers are not advised to back up their Private Keys used for Signing.

6.2.5 *Private Key archival*

Subscribers may make their own arrangement for archival of historical Private Keys used for encryption. Subscribers are not permitted to archive their Private Keys used for Signing as once the Certificate has expired, the Private Key for Signing is not required to determine that a message has been signed.

6.2.6 *Private Key entry into Cryptographic Module*

The Subscriber should ensure that their Private Keys are entered into a Cryptographic Module in an appropriate manner.

6.2.7 *Method of activating Private Key*

No stipulation.

6.2.8 *Method of deactivating Private Key*

No stipulation.

6.2.9 *Method of destroying Private Key*

Private Keys should 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*

No stipulation.

6.3.2 *Usage periods for the Public and Private Keys*

1. Unless earlier Revoked, the validity period of a Type 3 Certificate is one or two years. The validity period of a Type 3 Certificate can be determined by examining the “Valid From” and “Valid To” fields in the Certificate.
2. Subscribers shall cease all use of their Private Key for Signing after their Certificates have Expired.

6.4 Activation Data

Activation Data refers to data other than the Keys that are required to operate Cryptographic Modules (eg password and pins).

6.4.1 Activation Data generation and installation

Subscribers shall generate and use the Activation Data for their Private Keys so as to protect against the loss, theft, modification, unauthorised disclosure, or unauthorised use of the Private Keys.

6.4.2 Activation Data protection

See **section 6.4.1**.

6.4.3 Other aspects of Activation Data

To the extent Activation Data is transmitted, Subscribers shall protect the transmission of Activation Data for their Private Keys using methods that protect against the loss, theft, modification, unauthorised disclosure or unauthorised use of the Private Keys protected by such Activation Data.

6.5 Computer Security Controls

Details of the VeriSign CA's operations and systems used to provide computer security can be found in this section of the CPS.

6.6 Life Cycle Technical Controls

Details of the VeriSign CA's life cycle technical controls can be found in the CA Operations Manual.

6.7 Network Security Controls

Details of the VeriSign CA's network security controls can be found in this section of the CPS.

6.8 Cryptographic Module Engineering Controls

Details of the VeriSign CA's Cryptographic Module engineering controls can be found in this section of the CPS.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

The Certificate Profile for Type 3 Certificates is as follows:

Type	Value
Subject (Distinguished Name)	*[Example values in italics for full details see **section 3.1.1.3**.]* CN = *user defined eg CCF Email Gateway* OU = *user defined eg CCF R1 Trial* OU = *user defined eg XYZ Worldwide* O = *XYZ Ltd* S = *Vic* C = *AU*
Issuer (Distinguished Name)	CN = Gatekeeper Type 3 CA OU = Gatekeeper PKI OU = Terms of use at https://www.esign.com.au/GKRPA/ O = VeriSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	min RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss
Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	CA: FALSE Max Path Len: N/A (critical)
Key Usage	DigitalSignature, NonRepudiation, KeyEncipherment, DataEncipherment (critical)
Certificate Polices	OID: 1.2.36.88021603.333.2.8 (Certificate Policy) OID: 1.3.6.1.5.5.7.2.1 (Policy Qualifier) https://www.esign.com.au/GKRPA/
Netscape Cert Type	OID 2.16.840.1.113730.1.1 Value 03 02 07 80
Private Extension (ABN)	OID 1.2.36.1.333.1 Value <ABN number (IA5 String)>
CRL Distribution Point	URL=http://onsitecrl.esign.com.au/GatekeeperType3CA/LatestCRL.crl URL=ldap://directory.esign.com.au/cn=Gatekeeper Type 3 CA,ou=Terms of use at https://www.esign.com.au/GKRPA/,ou=Gatekeeper PKI,o=eSign Australia?certificaterevocationlist;binary
Authority Information Access	OID 1.3.6.1.5.5.7.48.1 (Online Certificate Status Protocol) URL=https://ocsp.esign.com.au
Subject Alt Name	*[Example value in italics]* RFC822 Name=*rsmith@xyz.com.au*
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

Some certificates issued between 24 April 2003 and 1st July 2004 may have the profile as follows:

Type	Value
Subject (Distinguished Name)	*[Example values in italics for full details see **section 3.1.1.3**.]* CN = *user defined eg CCF Email Gateway* OU = *user defined eg CCF R1 Trial* OU = *user defined eg XYZ Worldwide* O = *XYZ Ltd* S = *Vic* C = *AU*
Issuer (Distinguished Name)	CN = Gatekeeper Type 3 CA OU = Gatekeeper PKI OU = Terms of use at https://www.esign.com.au/GKRPA/ O = VeriSign Australia
Version	3
Serial Number	Serial number value
Signature Algorithm	md5 RSA
Public Key	min RSA 1024 bit key
Valid From	dd/mm/yy hh/mm/ss
Valid To	dd/mm/yy hh/mm/ss
Basic Constraints	CA: FALSE Max Path Len: N/A (critical)
Key Usage	DigitalSignature, NonRepudiation, KeyEncipherment, DataEncipherment (critical)
Certificate Polices	OID: 1.2.36.2038371.333.2.8 (Certificate Policy) OID: 1.3.6.1.5.5.7.2.1 (Policy Qualifier) https://www.esign.com.au/GKRPA/
Netscape Cert Type	OID 2.16.840.1.113730.1.1 Value 03 02 07 80
Private Extension (ABN)	OID 1.2.36.1.333.1 Value <ABN number (IA5 String)>
CRL Distribution Point	URL=http://onsitecrl.esign.com.au/GatekeeperType3CA/LatestCRL.crl URL=ldap://directory.esign.com.au/cn=Gatekeeper Type 3 CA,ou=Terms of use at https://www.esign.com.au/GKRPA/,ou=Gatekeeper PKI,o=eSign Australia?certificaterevocationlist;binary
Authority Information Access	OID 1.3.6.1.5.5.7.48.1 (Online Certificate Status Protocol) URL=https://ocsp.esign.com.au
Subject Alt Name	*[Example value in italics]* RFC822 Name=*rsmith@xyz.com.au*
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

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

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

7.1.3 Algorithm object identifiers

See this section in the CPS.

7.1.4 *Name forms*

Certificates Issued under this CP must contain the full Distinguished Name of the CA Issuing the Certificate in the "Issuer" field, and the Subscriber (and identify the Organisation) in the "Subject" field.

7.1.5 *Name Constraints*

See **section 3.1.1**.

7.1.6 *Certificate Policy Object Identifier*

The VeriSign CA supports the use of the Certificate Policy Object Identifier as is indicated in the Certificate Profile.

7.1.7 *Usage of Policy Constraints extension*

See this section in the CPS.

7.1.8 *Policy qualifiers syntax and semantics*

See this section in the CPS.

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

See this section in the CPS.

7.2.1 *Version number(s)*

See this section in the CPS.

7.2.2 *CRL and CRL entry extensions*

See this section in the CPS.

8 SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

1. The following process describes how changes to an Approved Document (including this CP and the CPS) 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 NOIE;

   (c) on determining that the change request is suitable for submission to NOIE, and that the changes required are clearly explained and documented, the Policy Approval Authority will forward a copy of the requested changes to NOIE 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 NOIE 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 accreditation 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 CP approval procedures

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