



SecureNet

SecureNet Limited

PO 01 - SecureNet Gatekeeper RCA-Issued Certificates Policy v1.0

No part of the contents of this document may be reproduced or distributed in any form or by any means without the prior written permission of SecureNet Limited.

Copyright © 1999-2002 SecureNet Limited
All Rights Reserved.

The information contained in this document is intended for SecureNet Limited personnel charged with the management and operation of the Certificate Authorities owned and operated as the SecureNet Trust Centre, those persons named as recipients, and Subscribers and Relying Parties using Certificates within the SecureNet Gatekeeper PKI Hierarchy.

Contact:

Operations Manager
SecureNet Limited
Locked Bag 32Pyrmont NSW 2009
AUSTRALIA

Table 1: Version History

Doc. Version	Status	Date of Issue	Issued By	Comments
0.1	Draft	11.06.02	JC	Re-branding from BCAPL to SecureNet, resetting of version numbers to 0.1 at NOIE/AGS request
0.2	Draft	24.08.02	JC, LO	Updates to align CP/CPS, and to reflect input from HIC, Telstra, and AGS.
0.3	Draft	10.09.02	JC,LO	Updates to reflect feedback from AGS.
0.4	Draft	12.09.02	JC,LO	Updates based on workshop with AGS, the Competent Authority.
0.5	Draft	18.09.02	JC,LO	Updates from workshop with AGS, NOIE, HIC/HeSA
0.6	Draft	23.09.02	LO	Changes to make distinction between SecureNet Gatekeeper RCA and SecureNet Enterprise RCA clear, minor editing changes, removal of address of RCA for security reasons, removal of references to NOIE with references to “the Competent Authority”, where relevant.
0.7	Draft	23.09.02	LO	Document updated to correct errors identified by Zakir Hussain.
0.8	Draft	25.09.02	AGS	AGS – proposed final amendments.

Doc. Version	Status	Date of Issue	Issued By	Comments
0.9A	Draft	01.10.02	AGS	AGS Final.
1.0	Final	10.10.02	NOIE	Accredited final

This Certificate Policy has been authorised by the SecureNet Policy Management Authority:

Date: _____

Chairperson

Date: _____

Audit/Accreditation Compliance

Date: _____

Operations Manager

Date: _____

Legal Counsel

Table of Contents

1.	Introduction	2
1.1	Overview	2
1.1.1	Standards	3
1.1.2	Definitions	4
1.1.3	X.500 Object Identifier hierarchy	4
1.1.4	Policy Qualifier	5
1.1.5	Gatekeeper Evaluation	5
1.2	Identification	5
1.2.1	SecureNet Gatekeeper RCA OID	5
1.2.2	SecureNet Gatekeeper RCA CP OID	5
1.3	Community and Applicability	6
1.3.1	Policy Authorities	6
1.3.2	Certification authorities	8
1.3.3	Registration Authorities	12
1.3.4	Subscribers	12
1.3.5	Relying Parties	12
1.3.6	Applicability	12
1.4	Contact Details	13
1.4.1	Specific administration organisation	13
1.4.2	Contact person	13
1.4.3	Person determining CPS suitability for this policy	13
2.	General Provisions	14
2.1	Obligations	14
2.1.1	SecureNet Obligations	14
2.1.2	CA Obligations	14
2.1.3	RA obligations	17
2.1.4	Subscriber obligations	17
2.1.5	Relying party obligations	19
2.1.6	Repository Obligations	19
2.2	Liability	20
2.2.1	CA Liability	20
2.2.2	RA Liability	21
2.2.3	Subscriber Liability	22
2.2.4	Relying Party Liability	22
2.2.5	Liability of the Commonwealth	22
2.3	Financial responsibility	23

2.3.1	Indemnification by Relying Parties	23
2.3.2	Fiduciary relationships.....	23
2.3.3	Administrative processes.....	23
2.4	Interpretation and Enforcement	23
2.4.1	Governing Law	23
2.4.2	Severability, survival, merger, notice, assignment	24
2.4.3	Dispute resolution procedures.....	26
2.5	Fees	28
2.5.1	Certificate issuance or renewal fees.....	28
2.5.2	Certificate access fees	28
2.5.3	Revocation or status information access fees.....	28
2.5.4	Fees for other services such as policy information.....	28
2.5.5	Refund policy.....	29
2.6	Publication and repository	29
2.6.1	Publication of RCA information.....	29
2.6.2	Frequency of publication	29
2.6.3	Access controls	30
2.6.4	Repositories.....	30
2.7	Compliance Audit	32
2.8	Data protection and privacy.....	33
2.8.1	Types of information to be protected	33
2.8.2	Types of information that may be disclosed.....	35
2.8.3	Disclosure of Certificate revocation/suspension information	36
2.8.4	Release to law enforcement officials.....	36
2.8.5	Release as part of civil discovery	37
2.8.6	Disclosure upon owner's request.....	37
2.8.7	Other information release circumstances	37
2.9	Intellectual Property Rights.....	37
2.9.1	General provision.....	37
3.	Identification and Authentication	39
3.1	Initial registration	39
3.1.1	Types of names.....	39
3.1.2	Need for names to be meaningful.....	39
3.1.3	Rules for interpreting various name forms.....	40
3.1.4	Uniqueness of names.....	40
3.1.5	Name claim dispute resolution procedure	40
3.1.6	Recognition, authentication and role of trademarks.....	40
3.1.7	Method to prove possession of Private Key.....	41
3.1.8	Identification and Verification – RCA	41
3.1.9	Identification and Verification – Client CA.....	42
3.1.10	Verification of Organisation Identity.....	42
3.1.11	Verification of Organisation Officer's Individual Identity.....	43

3.1.12	Verification of Officer’s Organisational Status.....	43
3.2	Routine Re-Key	43
3.2.1	CA Routine Re-Key.....	43
3.3	Re-key after Revocation.....	44
3.4	Revocation request	44
4.	Operational Requirements.....	46
4.1	Certificate Application	46
4.2	Certificate Issuance	46
4.2.1	Certificate issuance – SecureNet Gatekeeper RCA and OCA	46
4.2.2	Certificate issuance – Client CA.....	47
4.3	Certificate acceptance.....	48
4.4	Certificate suspension and revocation.....	48
4.4.1	General.....	48
4.4.2	Circumstances for revocation	49
4.4.3	Who can request revocation.....	51
4.4.4	Procedure for revocation request	51
4.4.5	Revocation request grace period.....	53
4.4.6	Circumstances for suspension.....	53
4.4.7	Who can request suspension	54
4.4.8	Procedures relating to suspension.....	54
4.4.9	Limits on suspension period.....	55
4.4.10	CRL issuance frequency	56
4.4.11	CRL checking requirements	56
4.4.12	On-Line revocation/status checking availability	56
4.4.13	On Line revocation checking requirements.....	56
4.4.14	Other forms of revocation advertisements available.....	56
4.4.15	Checking requirements for other forms of revocation advertisements.....	56
4.4.16	Special requirements re key compromise.....	56
4.5	Security Audit procedures	57
4.6	Records Archival	57
4.7	Key changeover.....	57
4.8	Compromise and Disaster Recovery.....	58
4.8.1	Computing resources, software, and/or data are corrupted.....	58
4.8.2	SecureNet CA Public Key is revoked.....	58
4.8.3	SecureNet CA Private Key is compromised.....	58
4.8.4	Secure facility after a natural or other type of disaster	59
4.8.5	Contingency & Disaster Recovery Plan.....	59
4.9	CA termination.....	59
4.9.1	Introduction.....	59
4.9.2	RCA Programmed Termination	60

4.9.3	CA Non-programmed Termination	62
4.9.4	Client CA Termination.....	63
4.9.5	Transfer of Root CA Data	63
5.	Physical, procedural, and personnel security controls	64
6.	Technical Security Controls	66
6.1	Key Pair Generation	66
6.1.1	Key pair generation	66
6.1.2	Private Key delivery to entity.....	66
6.1.3	Public Key delivery to Certificate issuer	66
6.1.4	CA Public Key delivery to users	66
6.1.5	Key sizes	67
6.1.6	Public Key parameters generation	67
6.1.7	Parameter quality checking.....	67
6.1.8	Hardware/software Key generation	67
6.1.9	Key usage purposes	67
6.2	Private Key Protection	68
6.2.1	Standards for cryptographic module.....	68
6.2.2	Private Key (n out of m) multi-person control.....	68
6.2.3	Private Key escrow	68
6.2.4	Private Key backup.....	68
6.2.5	Private Key archival	68
6.2.6	Private Key entry into cryptographic module.....	69
6.2.7	Method of activating Private Key.....	69
6.2.8	Method of deactivating Private Key	69
6.2.9	Method of destroying Private Key.....	69
6.3	Other Aspects of Key Pair Management.....	70
6.3.1	Public Key archival	70
6.3.2	Usage periods for the Public Keys and Private Keys	70
6.4	Activation Data	70
6.4.1	Activation data generation and installation	70
6.4.2	Activation data protection	70
6.4.3	Other aspects of activation data	71
6.5	Computer Security Controls.....	71
6.6	Life Cycle Technical Controls.....	71
6.7	Network security controls.....	71
6.8	Cryptographic module engineering controls.....	71
7.	Certificate and CRL Profiles	72
7.1	CA Certificate Profiles	72
7.1.1	Version number(s).....	72
7.1.2	Certificate extensions.....	72

7.1.3	Algorithm object identifiers	73
7.1.4	Name forms	74
7.1.5	Name constraints.....	74
7.1.6	Certificate policy Object Identifier	74
7.1.7	Usage of Policy Constraints extension.....	74
7.1.8	Policy qualifiers syntax and semantics	74
7.1.9	Processing semantics for the critical Certificate policy extension.....	74
7.2	CRL Profile	74
7.2.1	Version number(s).....	74
7.2.2	CRL and CRL entry extensions	75
8.	Specification Administration.....	76
8.1	Specification change procedures	76
8.1.1	Initial publication.....	76
8.1.2	Change.....	76
8.2	Publication and notification policies.....	77
8.3	CP approval procedures	77
9.	APPENDIX A.....	78
10.	APPENDIX B.....	80
11.	APPENDIX C.....	82

1. Introduction

1.1 Overview

1. SecureNet Limited (SecureNet) ACN 073665175 is a publicly listed company incorporated in Australia.
2. SecureNet, in its Gatekeeper Accredited role as a Certification Authority (CA) provides a range of services (PKI services) to support both Gatekeeper Accredited and non-Gatekeeper Accredited Public Key Infrastructure hierarchies (PKI Hierarchies). Non-Gatekeeper Accredited PKI Hierarchies are outside the scope of this Gatekeeper Approved Document.
3. The SecureNet Gatekeeper Root CA (referred to in this CP as the 'SecureNet Gatekeeper RCA') is the highest point of trust within the SecureNet Gatekeeper PKI Hierarchy. All other CA and RA entities in the SecureNet Gatekeeper PKI Hierarchy rely on this point of trust. The SecureNet RCA not only generates and signs its own Certificate, but certifies the Certificates of the Organisational CAs (OCAs) or industry-based Intermediate CAs (ICAs) subordinate to the SecureNet Gatekeeper RCA. These OCAs or ICAs may be branded as SecureNet entities, or as SecureNet client entities. In this Certificate Policy (CP), these OCAs and ICAs, including the SecureNet Gatekeeper OCA, are referred to as "Client CAs". All CAs and RAs in the SecureNet Gatekeeper PKI Hierarchy are Gatekeeper Accredited.
4. This Certificate Policy (referred to in this CP as the 'Gatekeeper RCA CP') relates to:
 - (a) the self-signed SecureNet Gatekeeper RCA authentication and confidentiality Certificates which the RCA issues to itself; and
 - (b) the authentication and confidentiality Certificates signed by the SecureNet Gatekeeper RCA and issued to Client CAs.

5. SecureNet conducts its Gatekeeper RCA role in accordance with the Approved Documents. The Approved Documents comprise:
- (a) the following public documents:
 - (i) SecureNet Gatekeeper Certificate Policies;
 - (ii) relevant Client CA Gatekeeper Certificate Policies;
 - (iii) the SecureNet Gatekeeper CPS; and
 - (iv) relevant Client CA or RA Gatekeeper CPS's; and
 - (b) the following confidential documents:
 - (i) PO 03 – Concept of Operations;
 - (ii) CO 02 – Gatekeeper CA Head Agreement;
 - (iii) SE 01 – Security Policy;
 - (iv) SE 02 – Protective Security Risk Review;
 - (v) SE 06 – Key Management Plan;
 - (vi) SE 04 – Protective Security Plan;
 - (vii) SE 03 – Disaster Recovery and Business Continuity Plan;
 - (viii) AD 01 – Certification Authority Operations Manual;
 - (ix) AD 01B – Configuration Baseline;
 - (x) SecureNet CA Services agreement.

Whilst the confidential documents are named in this CP, the contents are not disclosed for security reasons.

1.1.1 Standards

1. This CP is based on RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX RFC2527, by S. Chokhani and W. Ford, March 1999.

2. However, in some instances, this guideline does not provide adequate definition. In such cases, this CP will differ from the guideline insofar as is necessary for clarity only.

1.1.1.1 Certificate types issued

The SecureNet Gatekeeper RCA issues:

- (a) the self-signed RCA Certificate; and
- (b) Client CA Certificates.

1.1.2 Definitions

1. The definitions used within this document are published by SecureNet at:

<http://www.securenet.com.au>

2. These definitions are based on:
 - (a) ISO Glossary of IT Security Technology¹; and,
 - (b) Gatekeeper Glossary.²

1.1.3 X.500 Object Identifier hierarchy

1. Specified elements under this PKI have been assigned an X.500 Object Identifier (OID). The details of these OIDs are provided in the SecureNet document *AD 01C – X.500 Object Identifier Tree*, which is available from SecureNet.
2. The authority for issuing such object identifiers is the SecureNet PMA.

¹ Glossary of IT security terminology prepared by JTC1 SC 27 at <http://www.din.de/ni/sc27/doc6.html>

² Annex O of *Gatekeeper - a strategy for public key technology use in the Government* available from <http://www.govonline.gov.au/projects/publickey/GatekeeperAccreditation.htm>

1.1.4 Policy Qualifier

1. All SecureNet Gatekeeper RCA Certificates issued under this CP contain a 'policy qualifier', which summarises the major points of this CP. The purpose of the policy qualifier is to provide the person relying upon the Certificate with an abbreviated description of the main features of the CP under which the Certificate was issued.
2. Other fields in the Certificate provide details of where and how to find a complete copy of this CP.

1.1.4.1 Policy Qualifier – RCA

The text of the policy qualifier in all SecureNet Gatekeeper RCA-issued Certificates is:

Certificates under this policy are issued by the SecureNet Root CA to the RCA itself (self-signed) or to CAs subordinate to the RCA.

1.1.5 Gatekeeper Evaluation

SecureNet has been granted full accreditation by the Competent Authority following a successful evaluation by a team of Authorised Evaluators against the Gatekeeper Criteria for the Accreditation of Certification Authorities. These criteria may be found at:

<http://www.noie.gov.au>

1.2 Identification

1.2.1 SecureNet Gatekeeper RCA OID

The OID for the SecureNet Gatekeeper RCA is:

1.2.36.73665175.4

1.2.2 SecureNet Gatekeeper RCA CP OID

The OID for this policy is:

**RCA self-signed Certificates:
1.2.36.73665175.4.1**

**Client CA Certificates:
1.2.36.73665175.4.2**

1.3 Community and Applicability

1. The SecureNet Gatekeeper RCA is the highest point in the chain of trust within the SecureNet Gatekeeper PKI Hierarchy. It is the point on which all entities in the hierarchy ultimately rely. The SecureNet Gatekeeper RCA self-signed Certificate is used by Relying Parties to establish this chain of trust.
2. This RCA CP is applicable to:
 - (a) the SecureNet Gatekeeper RCA self-signed Certificate; and
 - (b) Client CA Certificates issued by the SecureNet Gatekeeper RCA.
3. All CAs and RAs within the SecureNet Gatekeeper PKI Hierarchy must be Gatekeeper Accredited.

1.3.1 Policy Authorities

Three policy approval authorities are relevant to this CP:

- (a) the Competent Authority;
- (b) the SecureNet Policy Management Authority (PMA); and
- (c) Client PMAs.

1.3.1.1 Competent Authority

NOIE is responsible for defining the high level criteria against which CAs and RAs are to be evaluated and, when successfully evaluated, CAs and RAs are Gatekeeper Accredited by the Competent Authority. Once accredited, a CA may offer and issue Certificates to Commonwealth Agencies, or to those organisations and entities with which the Agencies conduct electronic transactions.

1.3.1.1.1 Competent Authority Contact details

The contact details for the Competent Authority are:

Name:	CEO, NOIE
Postal Address:	GPO Box 390 Canberra ACT 2601 Australia
Phone:	+61 2 6271 1656
Fax:	+61 2 6271 1698
Domain	http://www.noie.gov.au

1.3.1.2 SecureNet Policy Management Authority (SecureNet PMA)

1. The SecureNet PMA sets out the overarching operational doctrine for the SecureNet Gatekeeper PKI Hierarchy.
2. The SecureNet PMA has the following functions:
 - (a) to give internal approval to CPs within the SecureNet Gatekeeper PKI Hierarchy;
 - (b) to approve the issue of a new RCA-Issued Certificate;
 - (c) to approve the establishment of Client PMAs;
 - (d) to administer policy infrastructure to maintain the integrity of the SecureNet Gatekeeper PKI Hierarchy.

1.3.1.2.1 SecureNet PMA Contact details

The contact details for the SecureNet PMA are:

Name:	SecureNet Limited
Contact:	Policy Management Authority
Title:	Operations Manager
ACN:	073665175
Postal Address:	Locked Bag 32 Pyrmont NSW 2009
Phone:	+61 2 8514 7300
Fax:	+61 2 8514 7301
E-mail Address:	info@securenet.com.au

1.3.1.3 Client Policy Management Authorities (PMA)

1. Client CAs shall operate a Client Policy Management Authority (PMA). Client PMAs are responsible for the creation and internal approval of policies which are unique to the operation of the Client CA.
2. The Client PMA performs the following functions:
 - (a) formulates and gives internal approval to new policy and policy changes within the Client CA policy domain;
 - (b) submits new or changed policies to the SecureNet PMA for internal approval prior to submission to the Competent Authority; and
 - (c) oversees and manages compliance with Gatekeeper Accreditation requirements within its own policy domain.

1.3.2 Certification authorities

1.3.2.1 SecureNet Gatekeeper RCA

1. The CA which issues Certificates binding the SecureNet Gatekeeper RCA and its Client CAs to their Public Keys is the SecureNet Gatekeeper RCA.

2. The postal address of the SecureNet Gatekeeper RCA is:

SecureNet Limited Locked Bag 32
Pymont NSW 2009

1.3.2.2 SecureNet Gatekeeper RCA Functions

The functions performed by the SecureNet Gatekeeper RCA are:

- (a) constitution of a PMA for the purposes of reviewing and providing internal approval for policies applicable to, and recognised by, the SecureNet Gatekeeper RCA;
- (b) approval of the naming conventions for the creation of distinguished names for Certificate applicants, in compliance with the X.500 standard for Distinguished Names;
- (c) generation of its own Keys using software that is listed on the DSD Evaluated Products List (EPL);
- (d) issuing to itself a self-signed Certificate binding the RCA to its own Public Key;
- (e) publication of the SecureNet Gatekeeper RCA Hash on the SecureNet Website at:

<http://www.securenet.com.au>

- (f) administration of the registration of Client CAs in accordance with the Certificate registration process described in this CP;
- (g) issuing to Client CAs signed Certificates binding Client CAs to their Public Keys;
- (h) publication of the Public Key Certificates it issues in the SecureNet X.500 Directory;
- (i) provision to Relying Parties of access to:
 - (i) Certificate information published in the SecureNet X.500 Directory; and
 - (ii) the Public Keys associated with operational Certificates that are listed in the SecureNet X.500 Directory;

- (j) operation of the SecureNet Gatekeeper RCA in an efficient and trustworthy manner and in accordance with the Approved Documents;
- (k) making reasonable inquiries to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level in the SecureNet Gatekeeper PKI Hierarchy;
- (l) revocation of Client CA Certificates in accordance with the Client CA Certificate revocation process described in this CP;
- (m) posting of details of revoked Client CA Certificates in the Certificate Revocation List (CRL) in the SecureNet X.500 Directory;
- (n) conduct of regular internal security audits;
- (o) facilitation of the conduct of regular audits by NOIE-authorized external auditors relating to the maintenance of Gatekeeper Accreditation status; and
- (p) conduct of compliance audits of Client CAs.

1.3.2.2.1 SecureNet Gatekeeper RCA Contact Details

The contact details for the SecureNet Gatekeeper RCA are:

Name:	SecureNet Limited
ACN:	073665175
OID:	1.2.36.73665175.4
Postal Address:	Locked Bag 32 Pymont NSW 2009
Phone:	+61 2 8514 7300
Fax:	+61 2 8514 7301
Domain Name:	http://www.securenet.com.au
E-mail Address:	info@securenet.com.au
Contact:	Operations Manager

1.3.2.3 Client Certification Authorities

The Registered Address of a Client CA can be found in the CP(s) of the Certificates it issues.

1.3.2.4 Client CA Functions

Functions performed by Client CAs under this CP include:

- (a) generating their own Keys;
- (b) submitting their Public Keys together with Certificate Requests to the SecureNet Gatekeeper RCA;
- (c) operating the Client CA in an efficient and trustworthy manner and in accordance with the Gatekeeper strategy and their own Approved Documents;
- (d) conducting regular internal security and accreditation audits; and
- (e) facilitating the conduct of regular audits by NOIE-authorized external auditors relating to the maintenance of Gatekeeper Accreditation status.

1.3.3 Registration Authorities

1. The identity of the SecureNet Gatekeeper RCA is confirmed by the SecureNet PMA using the procedures laid down in Section 3.1, of this CP (Initial registration).
2. The SecureNet Gatekeeper RCA is responsible for checking Evidence of Identity (EOI) and collecting Registration Information for and about Client CAs only.

1.3.4 Subscribers

1. For the purposes of this CP, the Subscribers are Client CAs.
2. The SecureNet Gatekeeper RCA does not issue Certificates to End Entities and does not check EOI or collect Registration Information for End Entities.

1.3.5 Relying Parties

For the purposes of this CP, a Relying Party is an entity who relies on a digital signature created by a Subscriber referred to in section 1.3.4, or who relies on a Certificate issued by the SecureNet Gatekeeper RCA under this CP.

1.3.6 Applicability

Certificates supported by this CP are limited to:

- (a) the self-signed SecureNet Gatekeeper RCA Certificate; and
- (b) Client CA Certificates issued by the SecureNet Gatekeeper RCA.

1.3.6.1 Applicable Certificate usage

1. Certificates issued to CAs under this CP are used to verify the chain of trust for all Client CAs within the SecureNet Gatekeeper PKI Hierarchy. In verifying Certificates in the chain of trust within the SecureNet Gatekeeper PKI Hierarchy, a Relying Party should take account of any limitations or limits on usage of those Certificates.
2. The SecureNet Gatekeeper RCA Certificate contains the SecureNet Gatekeeper RCA's Public Key and information about its validity.

1.4 Contact Details

1. Enquiries or other communications about this document should be addressed to:

**Operations Manager
SecureNet Limited
Locked Bag 32
Pymont NSW 2009**

2. E-mail may be sent to:

info@securenet.com.au

1.4.1 Specific administration organisation

This CP is administered by the SecureNet PMA.

1.4.2 Contact person

See Section 1.4, Contact Details.

1.4.3 Person determining CPS suitability for this policy

1. The Competent Authority and the SecureNet PMA have determined that the SecureNet CPS is suitable for this CP.
2. The Competent Authority and the organisations (including Organisations) which operate Client CAs or Client RAs are responsible for determining whether any relevant CPS is suitable for the relevant CP(s).

2. General Provisions

2.1 Obligations

This section covers the obligations of SecureNet (acting through its CAs) to all non-SecureNet PKI Entities in the SecureNet Gatekeeper PKI Hierarchy.

2.1.1 SecureNet Obligations

1. The SecureNet Gatekeeper RCA is the highest point of trust within the SecureNet Gatekeeper PKI Hierarchy.
2. SecureNet shall provide a certification infrastructure that enables the secure issue of Public Key Certificates to the SecureNet Gatekeeper RCA and Client CAs.

2.1.1.1 SecureNet PMA Obligations

1. The SecureNet PMA may propose amendments to this CP. Any changes to the CP must be approved by the Competent Authority.
2. The amended CP must be published on the SecureNet Website.
3. The SecureNet PMA shall:
 - (a) specify the time from which the new or amended CP will apply;
and
 - (b) consult with and notify NOIE and Client CAs prior to implementing any change to this CP.

2.1.2 CA Obligations

2.1.2.1 SecureNet Gatekeeper RCA Obligations

The SecureNet Gatekeeper RCA obligations are:

- (a) to comply with all Gatekeeper Approved Documents, Policies, Criteria and procedures;

- (b) to comply with applicable law;
- (c) to maintain the SecureNet Gatekeeper CPS and this CP;
- (d) to comply with, and ensure that its employees and contractors comply with, the conditions and obligations set out in this CP and the practices set out in the SecureNet CPS;
- (e) to advise Client CAs of their obligations under this CP and the SecureNet Gatekeeper CPS and make accessible a copy of this CP and the SecureNet Gatekeeper CPS to each Client CA;
- (f) to generate and issue Client CA Certificates only on receipt of properly formatted and verified Certificate Requests;
- (g) to ensure, at the time a Client CA Certificate is issued to a Client CA, that:
 - (i) the Client CA Certificate Information (i.e. information needed to complete a Client CA Certificate as required by the Certificate Profile) is accurate;
 - (ii) the Client CA Certificate contains all the elements required by the Certificate Profile (i.e. the specification of the fields to be included in a Client CA Certificate and the contents of each);
and
 - (iii) the Client CA is in possession or control of the Private Key corresponding to the Public Key included in the Client CA Certificate;
- (h) to issue Certificates that are factually correct from the information known to the SecureNet Gatekeeper RCA at the time of issue, and that are free from data entry errors;
- (i) to establish the SecureNet X.500 Directory to hold information pertaining to all Certificates issued under this CP;
- (j) to receive suspension and revocation requests and take appropriate action;

- (k) to make reasonable enquiries in accordance with the arrangements agreed with Client CAs to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level the SecureNet Gatekeeper RCA deems warranted in its chain of trust;
- (l) to promptly notify a Client CA in the event that the SecureNet Gatekeeper RCA initiates revocation of a Client CA's Certificate(s);
- (m) if appropriate, to issue a new Client CA Certificate to a Client CA whose Keys have been compromised, or are suspected to have been compromised, after receiving a properly formatted and verified request from the Client CA for a new Client CA Certificate;
- (n) to conduct compliance audits of Client CAs;
- (o) to facilitate the conduct of regular audits by NOIE-authorized external auditors to maintain Gatekeeper Accreditation status;
- (p) when the SecureNet Gatekeeper RCA generates Key Pairs, to ensure that each Key Pair can work as an operable pair of cryptographic Keys;
- (q) to revoke a CA Certificate as required by, and in accordance with, this CP; and
- (r) to register the revocation of the CA Certificate so that this information is readily available to a Relying Party.

2.1.2.2 Client CA Obligations

1. The obligations of Client CAs, as a CA within a SecureNet PKI Hierarchy, are dealt within the CP under which the Client CA issues Certificates.
2. The obligations of a Client CA when acting in the role of a Subscriber are set out at 2.1.4.
3. The obligations of a Client CA when acting in the role of a Relying Party are set out at 2.1.5.

2.1.3 RA obligations

The obligations of the SecureNet Gatekeeper RCA when registering Client CAs are:

- (a) to conduct the verification process described in Section 3 of this CP;
- (b) to ensure the accuracy and completeness of any part of the Certificate Information which is generated or compiled by the SecureNet Gatekeeper RCA;
- (c) to ensure that all relevant information concerning a Certificate is recorded (electronically or otherwise) for an appropriate period of time, and in particular, for the purpose of providing evidence of certification for the purposes of legal proceedings;
- (d) to promptly authenticate and respond to all requests for Certificate Revocation and Suspension;
- (e) to utilise Trustworthy Systems, procedures and human resources in performing its services; and
- (f) to comply with any other relevant RA obligations set out in this CP.

2.1.4 Subscriber obligations

1. For the purposes of this CP, Subscribers are Client CAs.
2. The obligations of Client CAs, when acting as Subscribers, are:
 - (a) to comply with the provisions of this CP and the SecureNet Gatekeeper CPS;
 - (b) to comply with and maintain their own Gatekeeper Approved Documents, Policies, Criteria and procedures;
 - (c) to comply with the applicable law;
 - (d) to maintain a Client PMA with the authority to represent the Organisation in matters relating to the Client CA;

- (e) to ensure that all information provided to the SecureNet Gatekeeper RCA in relation to their Key Pairs and Certificates is true and complete;
- (f) to ensure that their own Key Pairs are operable pairs of cryptographic Keys which meet the requirements of their own and SecureNet's Key Management Plan;
- (g) to keep their Private Keys secret;
- (h) to promptly notify the SecureNet Gatekeeper RCA in the event that the Client CA's Keys have been compromised, or are suspected of having been compromised;
- (i) to cooperate with compliance audits conducted by the SecureNet Gatekeeper RCA;
- (j) to immediately notify the SecureNet Gatekeeper RCA if the Client CA ceases to be Gatekeeper Accredited or an adverse audit finding has been made about their Gatekeeper compliance, or there is any other change to their Registration Information, or any other information provided to the SecureNet Gatekeeper RCA.
- (k) to use Trustworthy Systems in which only authorised persons can make entries and changes, information can be checked for authenticity, and any technical changes compromising security are apparent to the operator;
- (l) to employ personnel who possess the expert knowledge, experience, and qualifications necessary for the provision of certification services;
- (m) to apply administrative and management procedures which are appropriate for the activities being carried out;
- (n) to enter into appropriate agreements with their own Subscribers and Relying Parties which clearly outline End Entity obligations; and
- (o) to obtain appropriate insurance to cover the risk of liability for damages flowing from its provision of certification services.

3. The issuance of Certificates to End Entities as Subscribers is outside the scope of this CP. The obligations of End Entities as Subscribers are set out in the CP under which the End Entity's Certificate was issued.

2.1.5 Relying party obligations

1. Before relying on a Certificate, Relying Parties must:
 - (a) confirm the validity of the Certificate (including checking whether or not it has been revoked); and
 - (b) ascertain and comply with the purposes for which the Certificate was issued, and any other limitations on reliance of the Certificate which are specified in the Certificate or this CP.
2. If a Relying Party relies on a Certificate in circumstances where:
 - (a) the relevant Certificate is invalid, or has been revoked and notice of revocation has been published as required under section 2.6; or
 - (b) the purpose for which it was relied on was not within the purposes or limitations referred to in paragraph 1(b);the Relying Party does so at its own risk.

2.1.6 Repository Obligations

1. The SecureNet Gatekeeper RCA provides and maintains the operational infrastructure for the SecureNet X.500 Directory which provides repository functions in support of this CP.
2. The SecureNet Gatekeeper RCA shall ensure timely publication of the Certificates and CRLs it issues to the SecureNet X.500 Directory in accordance with the SecureNet Gatekeeper Approved Documents
3. Client CAs operating under the SecureNet Gatekeeper PKI Hierarchy may also post Certificates and CRLs to the SecureNet X.500 Directory Repository. In this case, the repository obligations of Client CAs are set out in the relevant Client CA CP.

2.2 Liability³

2.2.1 CA Liability

2.2.1.1 RCA Liability

1. SecureNet is liable under or in connection with this CP for the loss or damage an entity or legal or natural person suffers if:
 - (a) the SecureNet Gatekeeper RCA issued a Certificate under this CP;
 - (b) the SecureNet Gatekeeper RCA breached clause 2.1.2.1 (g), (p), (q) or (r) in respect of that Certificate; and
 - (c) the entity or person reasonably relied on that Certificate and as a result, suffered the loss or damage;

unless SecureNet proves that it did not act negligently when it breached the relevant clause or clauses.

2. Where:

- (a) by the operation of law, a contract is formed between SecureNet and the entity or person who relied on the Certificate; or
- (b) no contract is formed between SecureNet and the entity or person who relied on the Certificate, but the entity or person was aware of limitations of the kind described in clause 2.2.1.3 and 2.2.1.4 in relation to the Certificate;

SecureNet and the Relying Party agree that SecureNet is not liable under or in connection with this CP for loss or damage suffered by that entity or person which:

- (c) arose from reliance on the Certificate in circumstances that are outside the limitations placed on it under clause 1.3.6.1 of this CP, the relevant CP under which the Certificate was issued or any applicable Subscriber or Relying Party Agreement; or

³ The liability régime that applies to the activities conducted under this CP, and any documents or activities related to this CP, have been evaluated to ensure that it complies with NOIE's Gatekeeper Strategy Update 2/2002, but is otherwise not subject to evaluation by the Australian Government Solicitor or accreditation by the Competent Authority

- (d) exceeds the limit that is specified on, or in relation to, the Certificate pursuant to clause 2.2.1.3 or 2.2.1.4.
3. SecureNet is not liable for the operation of any Client CA (except the SecureNet Gatekeeper OCA), or any consequence of malfeasance, tort or contractual breach arising from the operation thereof, except to the extent that the Client CA was operating in accordance with this CP and if applicable, the SecureNet Gatekeeper CPS.
 4. The total liability of SecureNet to a person or entity in respect of any claim by that person or entity which arises under or in connection with this CP or the transactions contemplated by this CP is limited to \$10,000 per claim. This limitation does not apply in relation to liability for:
 - (a) personal injury, including sickness and death; or
 - (b) loss of, or damage to, tangible property.
 5. In no event shall SecureNet be liable in respect of any claim arising under or in connection with this CP or the transactions contemplated by this CP for any loss of profit, loss of data or indirect or consequential loss or damage incurred or suffered by any person or entity, whether or not the SecureNet was or should have been aware of the possibility of such loss or damage.

2.2.1.2 Client CA Liability

1. The liability of a Client CA under or in connection with this CP when acting in the role of a Subscriber is set out at 2.2.3.
2. The liability of a Client CA under or in connection with this CP when acting in the role of a Relying Party is set out at 2.2.4.

2.2.2 RA Liability

The liability of SecureNet under or in connection with this CP when registering Client CAs is covered in clause 2.2.1. of this CP.

2.2.3 Subscriber Liability

A Client CA who is a Subscriber for the purposes of this CP is liable under or in connection with this CP to the extent to which it causes loss or damage to another PKI Entity (including because it is negligent or has breached an obligation on it under this CP, or the SecureNet Gatekeeper CPS) which results in damages being recoverable against it under the general law.

2.2.4 Relying Party Liability

A person or entity who is a Relying Party for the purposes of this CP is liable under or in connection with this CP to the extent to which it causes loss or damage to another PKI Entity (including because it is negligent or has breached an obligation on it under the CP or CPS under which the Certificate was issued) which results in damages being recoverable against it under the general law.

2.2.5 Liability of the Commonwealth

Notwithstanding any other provisions of this CP, and whether Keys or Certificates are used in a transaction with an Agency or not:

- (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 Entities which are carried out under, or in relation to, this CP; or
 - (ii) if relevant, the services or products of a particular PKI Entity; 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, Liability), the Commonwealth disclaims any and all liability of any kind whatsoever 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; or
- (iii) a negligent act or omission of the Commonwealth.

2.3 Financial responsibility

2.3.1 Indemnification by Relying Parties

Reserved.

2.3.2 Fiduciary relationships

Issuing Certificates in accordance with this CP does not make SecureNet or the SecureNet Gatekeeper RCA an agent, fiduciary, trustee, or other representative of any Client CA.

2.3.3 Administrative processes

SecureNet has undergone a review by the Commonwealth of Australia acting through the Department of Finance and Administration and has been given Endorsed Supplier status.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

1. This CP is governed by the laws in force in the Australian Capital Territory, Australia.
2. All parties subject to this CP agree to submit to the jurisdiction of the courts having jurisdiction in the Australian Capital Territory.

2.4.1.1 Applicable contract structure

Additional contracts that underpin the policies and practices described in this CP include:

- (a) The Gatekeeper CA Head Agreement: Establishes a contractual relationship between SecureNet and the Commonwealth of Australia, represented by NOIE, for the provision of CA services under Gatekeeper; and

- (b) Any SecureNet-Client CA Agreement: Describes contractual arrangements under which SecureNet will enable a Client CA to operate.

2.4.1.2 Associated contract structure

Product Licensing Agreement: Describes the licence terms and conditions of products provided to Client CAs which enable the provision of PKI services.

2.4.2 Severability, survival, merger, notice, assignment

2.4.2.1 Severability

In the event that any one or more of the provisions of this CP shall for any reason be held to be invalid, illegal, or unenforceable at law, such unenforceability shall not affect any other provision, but this CP shall then be construed as if such unenforceable provision or provisions had never been contained herein, and insofar as possible, construed to maintain the original intent of this CP.

2.4.2.2 Survival (Continuing obligations)

Subject to the requirements of this CP, if the relationship between any of the PKI Entities expires or is terminated for any reason, any provisions of this CP that are necessary for the PKI Entities to exercise their rights and discharge their obligations and responsibilities to each other under this CP will survive that termination or expiration.

2.4.2.3 Merger

If the Private Key corresponding to the Public Key that is contained in a Certificate is compromised, or the expiration date of a Certificate is reached or passed, then the rights and obligations of the entities described in this CP are those described in this CP, the CPS and any other legally enforceable agreement between the entities.

2.4.2.4 Notice

1. A notice, consent, request or any other communication under this CP must be in one of the following forms:
 - (a) Electronic — provided that the notice has been digitally signed by the entity sending it, which entity is part of the SecureNet Gatekeeper PKI Hierarchy;

- (b) In writing — provided that the notice:
 - (i) is left at the address recorded for the entity in this or the Client CA's CP; or
 - (ii) is sent by prepaid post (airmail if posted to or from a place outside Australia) to the address recorded for the entity in this or the Client CA's CP; or
 - (iii) is sent by facsimile to the facsimile number recorded for the entity in this or the Client CA's CP.
- 2. A notice, consent, request or any other communication is deemed to be received:
 - (a) if sent electronically, at the time that the notice is received by the recipient's host machine, and only after the digital signature has been verified and authenticated;
 - (b) if delivered by hand, when it is actually delivered to the recipient;
 - (c) if sent by letter, three days after posting (seven days, if posted to or from a place outside Australia);
 - (d) if sent by facsimile, at the time of dispatch, provided the sender obtains a transmission report which confirms that the facsimile was successfully sent in its entirety to the facsimile number of the recipient.

2.4.2.4.1 Notice action

- 1. Notices under this CP will be issued by SecureNet for the following events:
 - (a) release of a Gatekeeper Accredited, or re-Accredited, CP;
 - (b) revocation of the SecureNet Gatekeeper RCA's or a Client CA's Certificates;
 - (c) renewal of the SecureNet Gatekeeper RCA's or a Client CA's Certificates.

2. Parties requiring publication or receipt of a notice under this CP are required to provide notice of:
 - (a) changes in their address including postal and email addresses;
 - (b) security compromises of their Private Key(s);
 - (c) changes in information which would change the basis upon which the Certificate has been issued; and,
 - (d) any other event pertinent to the maintenance of the provisions of this CP.

2.4.2.4.2 Notice acknowledgment

Specific acknowledgment of any notice is not required except as provided for under this CP.

2.4.2.5 Assignment and novation

SecureNet may not assign its rights or novate its obligations under this CP except:

- (a) to a Gatekeeper Accredited entity; and
- (b) with the prior agreement of NOIE.

2.4.3 Dispute resolution procedures

The dispute resolution provisions apply to any issue arising under this CP. This includes, but is not limited to:

- (a) differences between this CP and any other Gatekeeper Approved CPs;
- (b) contractual matters arising out of this CP; and
- (c) subject to this CP, privacy policy and practice impacted by or on this CP.

2.4.3.1 Hierarchy of Certificate policy

In the event that a dispute arises between parties in the SecureNet Gatekeeper PKI Hierarchy, the following order of precedence will apply:

- (a) where the subject of the dispute is covered by a contract other than the CP, then the contract (ie not the CP) shall prevail;
- (b) where the subject of the dispute is covered wholly within this CP, then this CP applies;
- (c) to the extent of any inconsistency between this CP and the SecureNet Gatekeeper CPS, this CP shall prevail.

2.4.3.2 Process

1. If a dispute arises in connection with this CP, the parties undertake in good faith to use all reasonable endeavours to settle the dispute by negotiation or mediation.
2. This process is not binding where the dispute is between two SecureNet-owned entities.
3. If the parties are not able to resolve a dispute within a reasonable time from the date the dispute first arises, then the parties shall agree to jointly appoint an independent arbitrator having appropriate qualifications and practical experience (Arbitrator), for the purpose of resolving the dispute and agree to be bound by the decision of that Arbitrator.
4. If the parties are not able to agree on an Arbitrator within 14 days from the date the parties agreed to appoint an Arbitrator, then the parties agree to appoint the person nominated by the President for the time being of the Australian Institute of Arbitrators. Either party may request the President of the Australian Institute of Arbitrators to make such a nomination.
5. The parties will promptly furnish to the Arbitrator (imposing appropriate obligations of confidentiality) all information reasonably requested by the Arbitrator relating to the dispute.

6. The Arbitrator will use all reasonable endeavours to render the Arbitrator's decision within 30 days following receipt of the information requested or, if this is not possible, as soon as practical thereafter, and the parties must co-operate fully with the Arbitrator to achieve this objective.
7. The parties will share equally the fees and expenses of the Arbitrator.
8. If a party does not think that the process described above is appropriate, the parties can agree a different process that is more suitable to the circumstances of the dispute.

2.5 Fees

2.5.1 Certificate issuance or renewal fees

Fees may be payable by Client CAs for the issue or renewal of Certificates. Where fees are payable, SecureNet must provide an up to date fee schedule to all its Client CAs. This may be done by publishing the fee schedule on the SecureNet Website or directly to the CA.

2.5.2 Certificate access fees

Fees may be payable by Client CAs for access to the SecureNet X.500 Directory for Certificate retrieval. Where fees are payable, SecureNet must provide an up to date fee schedule to all its Client CAs. This may be done by publishing the fee schedule on the SecureNet Website or directly to the CA.

2.5.3 Revocation or status information access fees

Fees may be payable by Client CAs for access to the SecureNet X.500 Directory for Certificate revocation or status information. Where fees are payable, SecureNet must provide an up to date fee schedule to all its Client CAs. This may be done by publishing the fee schedule on the SecureNet Website or directly to the CA.

2.5.4 Fees for other services such as policy information

1. No fee is to be levied for access to this CP or SecureNet Gatekeeper CPS via the Internet. Printed copies of this CP are available from SecureNet for a fee.

2. Fees may be payable by Client CAs for the revocation or suspension of Certificates. Where fees are payable, SecureNet must provide an up to date fee schedule to all its Client CAs. This may be done by publishing the fee schedule on the SecureNet Website or directly to the CA.

2.5.5 Refund policy

1. A refund policy may apply to nominated fees.
2. Any SecureNet refund policy will be published on the SecureNet Website or notified directly to the Client CA.

2.6 Publication and repository

2.6.1 Publication of RCA information

2.6.1.1 Electronic publication

This CP is published electronically in PDF format on the SecureNet Website.

2.6.1.2 Hard copy publication

Paper copies of this document are available from SecureNet, for a fee. Requests should be directed to:

**Operations Manager
SecureNet Limited
Locked Bag 32 Pyrmont NSW 2009**

2.6.2 Frequency of publication

Publication frequency is as follows:

- (a) New versions of this CP and the SecureNet Gatekeeper CPS are published promptly;
- (b) Certificates are published promptly following their generation and issue;
- (c) CRL Publication is in accordance with Section 4.4.10, CRL issuance frequency.

2.6.3 Access controls

1. There are no access controls on the reading of this CP or of the SecureNet Gatekeeper CPS on the SecureNet Website.
2. Access to Certificate information (including CRLs) within the SecureNet X.500 Directory is limited to a single name search enquiry.
3. Appropriate access controls are used to restrict to authorised personnel the ability to write to, or modify, these items.

2.6.4 Repositories

1. The repository for all Public Key Certificates and public user information is the SecureNet X.500 Directory.
2. The SecureNet X.500 Directory may be accessed via the SecureNet Website.

2.6.4.1 X.500 Directory functions

1. The SecureNet X.500 Directory is provided for the retention of information about Client CAs operating within the SecureNet Gatekeeper PKI Hierarchy.
2. The SecureNet X.500 Directory serves as a repository for a list of:
 - (a) active Certificates (new and renewed);
 - (b) suspended Certificates (CRL);
 - (c) revoked Certificates (CRL); and
 - (d) expired Certificates.
3. The SecureNet X.500 Directory shall not publish:
 - (a) reasons why a Certificate has been revoked, unless the revocation reason is:
 - (i) CA compromise, or key compromise in which case a disclosure shall be made that the Private Key has been compromised; and

(ii) cessation of operation, in which case prior disclosure of the termination shall be given; or

(b) any information pertaining to a Client CA that is not contained in the Certificate, unless the Client CA agrees to publish such information.

2.6.4.2 X.500 Directory contact details

The contact details for the SecureNet X.500 Directory are:

Name:	SecureNet Limited
ACN:	073665175
Postal Address:	Locked Bag 32 Pymont NSW 2009
Phone:	+61 2 8514 7300
Fax:	+61 2 8514 7301
Domain Name:	www.securenet.com.au
E-mail Address:	info@securenet.com.au
Contact:	Operations Manager

2.6.4.3 X.500 Directory availability

1. The SecureNet X.500 Directory will normally be available 7 days a week, 24 hours a day.
2. In the event of a disaster, an alternate X.500 Directory will be activated from within the SecureNet disaster recovery site.

2.6.4.4 Repository Publication

1. The SecureNet X.500 Directory promptly publishes new Certificates and changes in Certificate status, including revocation, notices of suspension and expiry.
2. The SecureNet X.500 Directory is published on the SecureNet Website.

2.6.4.5 CRL Publication

The SecureNet Gatekeeper RCA regularly publishes an CRL applicable to its policy domain(s).

2.7 Compliance Audit

The SecureNet Gatekeeper RCA and Client CAs are audited regularly (internal and external audits) to ensure that these elements of the SecureNet Gatekeeper PKI Hierarchy are operating in accordance with all documented and/or Gatekeeper Accredited procedures and policies. Full details about the types of audits conducted are spelt out in section 2.7 of the SecureNet Gatekeeper CPS, including:

- (a) Frequency of entity compliance audit;
- (b) Identity/qualifications of auditor;
- (c) Auditor's relationship to audited party;
- (d) Topics covered by audit;
- (e) Actions taken as a result of deficiency; and
- (f) Communication of results.

2.8 Data protection and privacy

2.8.1 Types of information to be protected

2.8.1.1 Personal information

1. In this section 2.8, the expressions:
 - Agency;
 - approved privacy code;
 - Commonwealth contract;
 - contracted service provider;
 - organisation;
 - Personal Information; and
 - State or Territory authority;have the same meaning as they have in the *Privacy Act 1988*.
2. If, in the course of providing PKI services, SecureNet collects Personal Information from Organisations and Organisation Officers, SecureNet agrees to comply with:
 - (a) where the PKI services are provided to or in relation to a Commonwealth Agency or a contracted service provider for a Commonwealth contract – the Information Privacy Principles contained in the *Privacy Act 1988*; or
 - (b) where the PKI services are provided to a State or Territory authority then:
 - (i) where a State or Territory legislative privacy regime is applicable to SecureNet as a contractor to that State or Territory authority – that regime; or
 - (ii) if, or to the extent that, there is no State or Territory legislative privacy regime that is applicable to SecureNet as a contractor to that State or Territory authority – any other privacy regime which that State or Territory authority requires SecureNet to comply with whether the requirement appears in a services contract or otherwise; or
 - (c) where the PKI services are provided to an organisation that is not a Commonwealth Agency, or a contracted services provider for a Commonwealth contract:
 - (i) the National Privacy Principles; or

(ii) any approved privacy code to which SecureNet is bound;
whichever is applicable.

3. SecureNet agrees to ensure that any subcontract entered into for the purpose of fulfilling its obligations under this CP in respect of a Commonwealth Agency contains provisions to ensure that the subcontractor has the same awareness and obligations as SecureNet has under this clause 2.8, including the requirement in relation to subcontracts.

2.8.1.2 Tax File Number legislation

Except as prescribed by relevant legislation, no tax file number is to be recorded or used for the purposes of Certificates issued under this CP.

2.8.1.3 Confidential Information

1. Confidential Information means information which by its nature is confidential and which the entity holding the information knows or should know is confidential, and includes the SecureNet documents set out at section 1.1 (Overview) para 5(b).
2. Each entity must protect Confidential Information it holds against unauthorised disclosure.
3. Some information provided to SecureNet will be another party's Confidential Information. Access to this Confidential Information by operational staff is on a need-to-know basis.
4. Paper based records and other documentation containing Confidential Information are kept in secure and locked containers or filing systems, separate from all other records.

2.8.1.4 Registration information

1. The SecureNet Gatekeeper RCA and OCA are registered by authorisation from the SecureNet PMA. As no evidence of identity information is required for SecureNet to register its own RCA or OCA, the official letter of authorisation shall constitute the Registration Information.

2. Client CA's provide Registration Information in accordance with section 3.1 of this CP. This Registration Information includes:
 - (a) Personal Information, which is protected in accordance with clause 2.8.1.1 of this CP;
 - (b) Confidential Information, which is to be protected in accordance with clause 2.8.1.3 of this CP; and
 - (c) Certificate Information, which can be disclosed in accordance with clause 2.8.2.1 of this CP.

2.8.1.5 Other protected information

Certain information provided to SecureNet will be protected under specific legislation, or guidelines made known to SecureNet. In relation to such information, SecureNet will protect that information in accordance with that legislation or those guidelines.

2.8.2 Types of information that may be disclosed

2.8.2.1 Certificate information

1. Certificate Information embodied in Certificates is not considered to be confidential.
2. As the SecureNet PMA authorises the creation of the SecureNet Gatekeeper RCA and OCA, the only information noted on the official letter of authorisation is the Certificate Information which will appear in the X.509 V3 Certificate.
3. This provision does not operate to prevent publication of Certificate Information.

2.8.2.2 Public Documents

The following SecureNet documents are public documents and are not considered to be Confidential Information:

- (a) AD 01C – X.500 Object Identifier Tree; and
- (b) the documents described in section 1.1 (Overview) para5(a).

2.8.3 Disclosure of Certificate revocation/suspension information

If the SecureNet Gatekeeper RCA Certificate or a Client CA Certificate is suspended, the Certificate will continue to be active but the CRL will show that the Certificate is suspended. During the period of suspension, no Relying Party should rely on Certificates issued under this Certificate.

2.8.3.1 Disclosure of Certificate suspension information

1. Information on the reasons for Certificate suspension will not be disclosed to any party.
2. The SecureNet X.500 Directory provides information indicating the fact of suspension but not the reason for suspension.

2.8.3.2 Disclosure of Certificate revocation information

1. Client CA Certificate revocation information is contained in an CRL which is publicly available via the SecureNet X.500 Directory.
2. Where the SecureNet Gatekeeper RCA Certificate is revoked, all Client CAs are notified.
3. Information considered in making a decision to revoke a Certificate will not be disclosed by SecureNet — only the fact of revocation and a standard reason code will be disclosed through the SecureNet X.500 Directory.

2.8.4 Release to law enforcement officials

No document or record belonging to or held by any entity in the SecureNet Gatekeeper PKI Hierarchy will be released to law enforcement agencies or officials except where:

- (a) a properly constituted warrant is produced or the information is otherwise legally required to be disclosed; and,
- (b) the law enforcement official is properly identified.

2.8.5 Release as part of civil discovery

No document or record belonging to or held by any entity in the SecureNet Gatekeeper PKI Hierarchy will be released to any person except where:

- (a) a properly constituted instrument that has emanated from a court having jurisdiction or an authority having legal jurisdiction (e.g. the Australian Securities and Investment Commission) requiring production of the information is produced; and,
- (b) the person requiring production is a person authorised to do so.

2.8.6 Disclosure upon owner's request

1. The subject of Registration Information has full access to that information, and is empowered to authorise release of that information to another party. A person will not have access to any subject's Registration Information unless formal authorisation is given by the subject.
2. Formal authorisation may take two forms:
 - (a) a properly constituted electronic request providing that the request is digitally signed by a Private Key associated with a valid Certificate issued under a SecureNet PMA-approved CP; or,
 - (b) by application in writing.
3. No release of Registration Information is permitted without formal authorisation in accordance with this section.

2.8.7 Other information release circumstances

No other release of information is permitted unless required by law.

2.9 Intellectual Property Rights

2.9.1 General provision

1. SecureNet warrants that it is in possession of, or holds, licences for the use of, hardware and software in support of this CP, and that use of this CP does not infringe any Intellectual Property Rights (IP Rights) of any third party.

2. The use of RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX RFC2527, by S. Chokhani and W. Ford, March 1999, for drafting this CP is acknowledged. The use of the Commonwealth Government's Gatekeeper policy and documentation is also acknowledged.
3. Unless otherwise agreed between the relevant parties (in a CP or otherwise):
 - (a) IP Rights in the SecureNet Approved Documents, the SecureNet Certificate Repository and CRLs for Certificates issued under this CP are owned by SecureNet;
 - (b) Copyright in the Object Identifiers (OID) for the SecureNet Gatekeeper PKI Hierarchy vest solely in SecureNet, and OIDs are not to be copied, used or otherwise dealt with in any way except as approved by the SecureNet PMA.
 - (c) IP Rights including all copyright in all Certificates belongs to, and will remain the property of, the CA that issued them, subject to any pre-existing IP Rights which may exist in the Certificates or the Certificate Information;
 - (d) SecureNet grants to all End Entities the right to use any Certificate issued by any CA in the SecureNet Gatekeeper PKI Hierarchy for the purposes for which they were issued;
 - (e) SecureNet hereby assigns any IP Rights in a Client CA's Distinguished Name to the Client CA; and
 - (f) any IP Rights in Key Pairs are owned by the entity which generated the Key Pair.

2.9.1.1 Distinguished names

1. SecureNet is the owner of all IP Rights in any Distinguished Name:
 - (a) created by one of its CAs; and
 - (b) in which the SecureNet name is used.
2. SecureNet hereby assigns to each Client CA any IP Rights which SecureNet has in any Distinguished Name created by the SecureNet Gatekeeper RCA which includes the relevant Client CA's name.

3. Identification and Authentication

3.1 Initial registration

1. The authorisation for the SecureNet Gatekeeper RCA to certify itself is given in the form of a letter from the SecureNet PMA to the SecureNet Operations Manager which outlines all the information required by the SecureNet Gatekeeper RCA to issue the SecureNet Gatekeeper RCA self signed Certificate.
2. The purpose of the registration process in relation to a Client CA is to establish the identity of an Organisation which owns the Client CA and the authority of that Client CA to provide certification services on behalf of the Organisation. In order to achieve this, the SecureNet Gatekeeper RCA collects Evidence of Identity in accordance with this section, and obtains proof of ownership of the Client CA's Private Keys.
3. Internal approval for the certification of Client CAs is given by the SecureNet PMA once the Client CA's Certificate application has been approved by the SecureNet PMA and the identification process has been successfully completed in accordance with this CP.

3.1.1 Types of names

1. Distinguished Names within the SecureNet Gatekeeper PKI Hierarchy comply with the X.520 Certificate standard.
2. The distinguished name for the SecureNet Gatekeeper RCA is:

Common Name:	SecureNet Gatekeeper Root CA
Organisation:	SecureNet Limited
Organisational Unit:	Trust Centre
Country:	AU

3.1.2 Need for names to be meaningful

Distinguished Names shall be meaningful.

3.1.3 Rules for interpreting various name forms

Distinguished Names shall include each of the elements specified in X.509.

3.1.4 Uniqueness of names

Each Distinguished Name assigned by the SecureNet Gatekeeper RCA to a Client CA within the SecureNet Gatekeeper PKI Hierarchy shall be unique.

3.1.5 Name claim dispute resolution procedure

1. The SecureNet Gatekeeper RCA shall resolve any Client CA name collisions brought to its attention.
2. Disputes regarding assignment of Distinguished Names shall be resolved under section 2.4.3.

3.1.6 Recognition, authentication and role of trademarks

1. Trademark rights or other IP Rights may exist in the Client CA Organisation's name, or other parts of the Registration Information or Certificate Information provided by or on behalf of the Client CA.
2. By applying for registration, the Client CA Organisation:
 - (a) authorises SecureNet to use the relevant IP for the purpose of creating a Distinguished Name and for other purposes reasonably necessary in relation to issue of Client CA Certificates to the Client CA;
 - (b) warrants that it is entitled to use that IP for the purposes for which Client CA Certificates are issued and may be used, without infringing the rights of any other person; and
 - (c) agrees to indemnify SecureNet against loss, damage, costs or expenses of any kind SecureNet incurs in relation to any claim, suit or demand against SecureNet in respect of an infringement or alleged infringement of the IP Rights of any person.

3. SecureNet may include the relevant IP as part of a Distinguished Name on the basis of the authorisation and warranty given above, and is not required to independently check the status of any trade mark or other IP Rights.

3.1.7 Method to prove possession of Private Key

1. The SecureNet Gatekeeper RCA must satisfy itself that the RCA Private Key in its possession does in fact correspond to the RCA Public Key in its self-signed Certificate. This assurance is provided by the use of an Evaluated Product for Key Pair generation and Public Key certification.
2. The SecureNet Key Management Plan specifies the means by which SecureNet establishes, at the time the Client CA Certificate is issued to the Client CA, that the Client CA is in possession of the Private Key corresponding to the Public Key included in the Certificate. This is done by an audited transfer of the Client CA public key to the SecureNet Gatekeeper RCA for signing immediately after Key Pair generation.
3. The detail of these processes is also contained in the script for the Key Generation Ceremony for the SecureNet Gatekeeper RCA or Client CA.

3.1.8 Identification and Verification – RCA

1. As the SecureNet Gatekeeper RCA Certificate is self-signed, Evidence Of Identity is not required.
2. Before generating a SecureNet Gatekeeper RCA self-signed Certificate, the SecureNet Operations Manager shall verify that authorisation has been granted by the SecureNet PMA.
3. The SecureNet Operations Manager's identity and organisational status is verified by confirming the Operations Manager's SecureNet Identity Card (photo ID).

3.1.9 Identification and Verification – Client CA

1. As the SecureNet Gatekeeper OCA's Certificate is issued by the SecureNet Gatekeeper RCA, the requirements for identification and verification of the SecureNet Gatekeeper OCA are the same as those for the SecureNet Gatekeeper RCA.
2. For a Client CA other than the SecureNet Gatekeeper OCA, a Certificate application by an Organisation Officer on behalf of an Organisation is processed as follows:
 - (a) To ensure the Organisation is a real entity, the SecureNet Gatekeeper RCA verifies the identity of the Organisation, under section 3.1.10;
 - (b) To ensure the Organisation Officer is authorised to create a CA and apply for a Client CA Certificate on behalf of the Organisation, the SecureNet Gatekeeper RCA shall:
 - (i) verify the identity of the Organisation Officer, under section 3.1.11; and
 - (ii) verify the authority of the Organisation Officer to apply on behalf of the Organisation, under section 3.1.12.

3.1.10 Verification of Organisation Identity

For Client CAs other than the SecureNet Gatekeeper OCA, Organisations shall produce Evidence Of Identity as follows:

- (a) if the Organisation is registered by a government authority - a Certificate or extract of registration produced by that authority, or a certified copy of such a Certificate or extract; or
- (b) if the Organisation is not registered by any government authority - a Constitution, Trust Deed, Partnership Deed or other document which establishes the Organisation, or
- (c) if the Organisation is an Agency, the administrative arrangement order evidencing the existence of the Agency, or the statutory instrument establishing the Agency.

3.1.11 Verification of Organisation Officer's Individual Identity

For Client CAs other than the SecureNet Gatekeeper OCA, an Organisation Officer who applies for a Client CA Certificate shall attend the SecureNet Gatekeeper RCA in person and produce personal evidence of identity in accordance with the Identification Record for a Signatory to an Account - 150 Points, prescribed under the Financial Transaction Reports Act 1998 (Commonwealth).

3.1.12 Verification of Officer's Organisational Status

For Client CAs other than the SecureNet Gatekeeper OCA, an Organisation Officer shall produce evidence that he or she is authorised to apply for a Client CA Certificate on behalf of the Organisation. Acceptable forms of evidence of authority are:

- (a) a letter of authority which is signed in a manner legally sufficient to bind the Organisation; or
- (b) a letter of authority signed by another person on behalf of the Organisation AND evidence that the signer has authority to bind the Organisation.

3.2 Routine Re-Key

3.2.1 CA Routine Re-Key

3.2.1.1 SecureNet Gatekeeper RCA and OCA Re-Key

The SecureNet Gatekeeper RCA or SecureNet Gatekeeper OCA may be issued with new Keys and Certificates on expiry of their current Certificates without re-checking the authorisation of the SecureNet PMA if:

- (a) the Certificates are valid (i.e. not expired) at the time the routine re-key falls due;
- (b) the SecureNet Gatekeeper RCA or OCA identification details have not changed; and
- (c) the SecureNet Gatekeeper RCA's or OCA's Private Keys have not been compromised.

3.2.1.2 Client CA Re-Key

A Client CA other than the SecureNet Gatekeeper OCA may be issued with new Keys and Certificates on expiry of its current Certificates without re-checking the identity of the Organisation or the identity and organisational status of the Organisational Officer, if:

- (a) the Client CA Certificates are valid (i.e. not expired) at the time the routine re-key falls due;
- (b) the Client CA's identification details have not changed; and
- (c) the Client CA's Private Key has not been compromised.

3.3 Re-key after Revocation

1. After revocation of a SecureNet Gatekeeper RCA or OCA Certificate, re-keying is by way of a new letter of authorisation prepared and approved by the relevant PMA.
2. For Client CAs other than the SecureNet Gatekeeper OCA, re-keying after revocation of a Client CA Certificate is by way of a Certificate application processed as for the initial registration.

3.4 Revocation request

1. A request to revoke the Certificate of the SecureNet Gatekeeper RCA or a Client CA is made in accordance with Section 4.4.4, Procedure for revocation request.
2. Before processing a request for Revocation of a Client CA Certificate other than a SecureNet Gatekeeper OCA Certificate, the SecureNet Gatekeeper RCA shall verify that the request is made by a person or entity authorised to request Revocation of that Certificate under section 4.4.3.
3. Acceptable forms of verification include:
 - (a) the request is digitally signed with a Private Key issued to an Organisation Officer under a SecureNet PMA – approved CP;
 - (b) the request is made in person and the identity of the requestor is verified as required under section 3.1.11; or

- (c) the request is made using a passphrase or similar security measure provided by the SecureNet Gatekeeper RCA.
4. The SecureNet Gatekeeper RCA procedure for verifying Revocation requests shall be set out in *AD 01 - Certification Authority Operations Manual*.

4. Operational Requirements

4.1 Certificate Application

1. A Certificate application for the SecureNet Gatekeeper RCA and SecureNet Gatekeeper OCA is approved by the unanimous resolution of the SecureNet PMA.
2. An organisation which is Gatekeeper Accredited and which wishes to join the SecureNet Gatekeeper PKI Hierarchy shall apply in writing to the SecureNet PMA for a Client CA Certificate to be issued to its Client CA, using the form of Certificate application as set out at Appendix A.
3. The SecureNet PMA will take reasonable care in accepting and processing Certificate applications. It will ensure that the practices described in this CP and the SecureNet Gatekeeper CPS are complied with and either approve or reject the Certificate application, as appropriate.
4. The SecureNet PMA may reject a Certificate application for any reason, or no reason.

4.2 Certificate Issuance

4.2.1 Certificate issuance – SecureNet Gatekeeper RCA and OCA

1. The SecureNet Gatekeeper RCA self-signed Certificate and SecureNet Gatekeeper OCA Certificate are generated and issued promptly on receipt of a letter of authorisation from the SecureNet PMA.
2. In response to an authorisation under paragraph 1, the SecureNet Gatekeeper RCA shall follow the procedures specified in the SecureNet Key Management Plan, and where applicable, the script for the SecureNet Gatekeeper RCA or OCA Key Generation Ceremony, to issue the associated Certificate.

3. As the SecureNet Gatekeeper RCA Certificate is a self-signed Certificate, a Certificate Request file is not needed. Using the software application, the Certificate Information is entered into the software and the Keys and self-signed Certificate are generated using that information. The Private Key is then backed up for secure archival offsite and is security sealed and recorded in the Trusted Element register. On expiry of the SecureNet Gatekeeper RCA Certificate, the backup copy of the Private Key is destroyed but the Public Key Certificate is archived for another 7 years from the date of expiry.
4. The SecureNet Gatekeeper RCA Key Generation Ceremony, requires, at a minimum, the following people to witness the event:
 - (a) one member of the SecureNet PMA; and
 - (b) one independent witness.
5. All witnesses must complete a Certificate Witness Statement which certifies that they witnessed the Certificate generation and are satisfied that the Certificate meets the agreed structure defined in the script for the Key Generation Ceremony.

4.2.2 Certificate issuance – Client CA

1. For Client CAs other than for the SecureNet Gatekeeper OCA, a SecureNet CA Services Agreement setting out the responsibilities of the Organisation, the Organisation Officer and SecureNet, and obliging the Client CA to comply with this CP, and the SecureNet Gatekeeper CPS, shall be executed by SecureNet and the Organisation, using handwritten signatures, before the SecureNet PMA authorises issuance of a Client CA Certificate to the Client CA.
2. Before commencing operations, a Client CA that has been approved by the SecureNet PMA for participation in the SecureNet Gatekeeper PKI Hierarchy, will require its Client CA Certificate to be generated and issued by the SecureNet Gatekeeper RCA.
3. In response to a request under paragraph 1, the SecureNet Gatekeeper RCA shall follow the procedures specified in the Client CA Key Management Plan, and where applicable, the script for the Client CA Key Generation Ceremony, to issue the Client CA Certificate.

4. Client CA Certificate Requests are securely submitted to the SecureNet Gatekeeper RCA by Client CAs in the form of Client CA Certificate Request files. Client CA Certificates will not be issued, or signed by the SecureNet Gatekeeper RCA, until the processes set out in this CP and SecureNet Gatekeeper CPS have been completed successfully. Once the Client CA Certificate is signed, it is securely returned to the Client CA for installation on the Client CA.

4.3 Certificate acceptance

1. The SecureNet Gatekeeper RCA's self-signed Certificate is deemed to have been accepted when the witnesses to the Key Generation Ceremony have signed their witness statements and certified that all information in the Certificate is correct.
2. A Client CA's use of its Private Keys or its Public Key Certificates, constitutes Client CA Certificate acceptance. Once a Client CA has accepted its Certificate, the Client CA is required to comply with its obligations under this CP and any other Approved Documents the Organisation has agreed to be bound by.
3. By accepting a Client CA Certificate, the Organisation also:
 - (a) agrees to be bound by the continuing responsibilities, obligations and duties imposed on them by their Gatekeeper Accreditation;
 - (b) represents and warrants that to its knowledge, no unauthorised person has had access to the Private Key associated with the Client CA Certificate; and
 - (c) represents and warrants that the Registration Information it supplied during the registration process is accurate, and the Certificate Information published in the Client CA Certificate is also accurate.

4.4 Certificate suspension and revocation

4.4.1 General

The prompt validation and actioning of a Certificate suspension or revocation request is central to the maintenance of the integrity of the SecureNet Gatekeeper PKI Hierarchy.

4.4.1.1 SecureNet Gatekeeper RCA Certificate Revocation

1. On receipt by the SecureNet PMA of a request to revoke the SecureNet Gatekeeper RCA self-signed Certificate, the SecureNet PMA shall meet immediately to verify the validity of the request.
2. If a request to revoke the SecureNet Gatekeeper RCA Certificate is verified:
 - (a) the SecureNet PMA will instruct the SecureNet Gatekeeper RCA via the SecureNet Operations Manager to suspend (but not revoke) the SecureNet Gatekeeper RCA Certificate forthwith. The SecureNet PMA will then inform NOIE of the suspension;
 - (b) subsequent to such suspension, the SecureNet PMA shall consult with NOIE to decide the best course of action. Possible actions are revocation of the SecureNet Gatekeeper RCA Certificate or lifting of the suspension; and
 - (c) in the event that a revocation is required, the SecureNet Gatekeeper RCA shall inform all Client CAs.

4.4.1.2 Client CA Certificate Revocation

If a properly formatted Request to revoke a Client CA Certificate is authenticated, and has been made in accordance with the provisions of this CP, the Certificate will be immediately revoked.

4.4.2 Circumstances for revocation

4.4.2.1 SecureNet Gatekeeper RCA and OCA Certificate Revocation

A SecureNet Gatekeeper RCA Certificate is revoked in the event of:

- (a) the theft, loss, disclosure, modification, or other compromise or suspected compromise of the SecureNet Gatekeeper RCA Private Key(s); or
- (b) the deliberate misuse by a trusted user of the SecureNet Gatekeeper RCA Private Keys and Certificates, or a substantial non-observance of operational requirements of this CP or of the practices in the SecureNet Gatekeeper CPS; or
- (c) the cessation of operation of the SecureNet Gatekeeper RCA; or

- (d) the improper or faulty issuance of the SecureNet Gatekeeper RCA Certificate; or
- (e) material SecureNet Gatekeeper RCA Certificate Information becoming inaccurate; or
- (f) a properly formatted request being received from the SecureNet PMA (for the SecureNet Gatekeeper RCA); or
- (g) a validated request for revocation being received from an Authorised Third Party.

4.4.2.2 Client CA Certificate Revocation

1. For Client CAs other than the SecureNet Gatekeeper OCA, the SecureNet Gatekeeper RCA shall revoke a Certificate on receipt of a request under section 4.4.2, verified as required by section 3.4.
2. The SecureNet Gatekeeper RCA shall revoke a Client CA Certificate (whether or not it has received a request to do so) if:
 - (a) the SecureNet PMA believes it is reasonably likely that the relevant Client CA Private Key has been compromised;
 - (b) faulty or improper Registration, Key Generation or Client CA Certificate Issuance has occurred;
 - (c) a Client CA ceases to hold Gatekeeper Accreditation;
 - (d) the Client CA ceases to operate; or
 - (e) the Client CA terminates its involvement in the SecureNet Gatekeeper PKI Hierarchy.
3. The SecureNet Gatekeeper RCA may also revoke a Client CA Certificate:
 - (a) if a Client CA has not complied with any significant obligation under this CP or any SecureNet-Client CA agreement, or
 - (b) in any other circumstances where the SecureNet PMA reasonably considers Revocation to be appropriate.

4. The SecureNet Gatekeeper RCA is not required to investigate any of the circumstances surrounding Revocation, but where it does decide to investigate the circumstances, it shall use reasonable endeavours to notify the Client CA beforehand of that intention.

4.4.3 Who can request revocation

1. Revocation of the SecureNet Gatekeeper RCA's Certificate can be initiated by:
 - (a) the SecureNet PMA; or
 - (b) an Authorised Third Party; or
 - (c) the Competent Authority.
2. Client CA Certificate Revocation can be initiated by:
 - (a) the Organisation Officer of the Client CA;
 - (b) the SecureNet PMA, under the circumstances described in 4.4.1.2;
 - (c) an entity which, as part of the Registration Information, certified or provided material evidence which comprised the Registration Information, on the grounds that the relevant information has changed; or
 - (d) an Authorised Third Party.

4.4.4 Procedure for revocation request

4.4.4.1 SecureNet Gatekeeper RCA Certificate Revocation

1. Revocation of the SecureNet Gatekeeper RCA's Certificate can only be initiated:
 - (a) after consultation with NOIE; and
 - (b) after the SecureNet PMA has met and a resolution has been made to revoke the SecureNet Gatekeeper RCA's Certificate; and
 - (c) a written authorisation to revoke the SecureNet Gatekeeper RCA's Certificate has been issued by the SecureNet PMA to the SecureNet Operations Manager.

2. Once the written authorisation is received by the SecureNet Operations Manager, the SecureNet Gatekeeper RCA Certificate is revoked by that person and:
 - (a) the SecureNet Gatekeeper RCA Certificate is added to the CRL in the SecureNet X.500 Directory; and
 - (b) all Client CAs are notified immediately by the SecureNet Gatekeeper RCA.

4.4.4.2 Client CA Certificate Revocation

1. A Certificate Revocation request, whether in paper or electronic form, is to contain the information in the SecureNet Revocation Request form set out at Appendix C.
2. A request to revoke a Certificate shall identify the Certificate to be revoked, explain the reason for revocation, and provide the information required to allow the request to be authenticated (e.g., digitally or manually signed).
3. The verification requirements for Revocation requests from Client CAs are the same as for Certificate application, and because of these requirements, such requests shall be delivered to the SecureNet Gatekeeper RCA either in the form of digitally signed file, or out-of-band, using one of the out-of-band methods provided for in 2.4.2.4 of this CP.
4. The SecureNet Gatekeeper RCA receives and authenticates the request, and for Client CAs other than the SecureNet Gatekeeper OCA, notifies the SecureNet PMA that a request for revocation has been received.
5. The SecureNet PMA may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation, and if the need is verified will direct the SecureNet Gatekeeper RCA to revoke the Client CA Certificate.
6. On receipt of the direction from the SecureNet PMA, the SecureNet Gatekeeper RCA will
 - (a) ensure the Client CA Certificate and Public Key are current;

- (b) prioritise the Revocation according to the time the Revocation requirement was identified;
 - (c) revoke the Client CA Certificate;
 - (d) place the serial number of the Certificate, and other identifying information on an CRL and then post the CRL in the SecureNet Repository; and
 - (e) issue a notice to the Client CA Certificate owner containing the Client CA Certificate details and the date and time of Revocation.
7. Information about a revoked Client CA Certificate shall remain in the CRL until the Client CA Certificate expires and for one additional CRL beyond that point.
8. The SecureNet PMA, at its discretion, may set out emergency procedures for the SecureNet Gatekeeper RCA to use to effect immediate revocation of a Client CA Certificate in the appropriate circumstances.

4.4.5 Revocation request grace period

1. No grace period is allowed for revocation of the SecureNet Gatekeeper RCA Certificate. As soon as the SecureNet PMA authorises such a revocation, it is actioned.
2. Revocation requests for Client CA Certificates are verified on receipt, and processed in priority order. There is no Revocation grace period.

4.4.6 Circumstances for suspension

1. The SecureNet Gatekeeper RCA's Certificate is suspended by the SecureNet Gatekeeper RCA when:
 - (a) the SecureNet PMA has reasonable grounds for believing that the SecureNet Gatekeeper RCA's Private Key has been compromised;
or
 - (b) the SecureNet PMA has reasonable grounds for believing that the media holding the SecureNet Gatekeeper RCA's Private Key is compromised; or

- (c) a properly formatted request is received in accordance with Section 4.4.8, (Procedures relating to suspension).
2. A Client CA Certificate may be Suspended if circumstances justifying Revocation are suspected, but unconfirmed.
3. A Client CA may request suspension of its Client CA Certificate for any reason, or for no reason.

4.4.7 Who can request suspension

1. Suspension of a SecureNet Gatekeeper RCA or SecureNet Gatekeeper OCA Certificate may be initiated by:
 - (a) the SecureNet PMA;
 - (b) the Competent Authority; or
 - (c) An Authorised Third Party.
2. For Client CAs other than the SecureNet Gatekeeper OCA, Certificate Suspension can be initiated by:
 - (a) the SecureNet PMA;
 - (b) the Organisation Officer of the Client CA; or
 - (c) an Authorised Third Party.

4.4.8 Procedures relating to suspension

1. A Certificate suspension request, whether in paper or electronic form, is to contain the information in the SecureNet Suspension Request form set out at Appendix B of this CP.
2. To process a suspension request, the SecureNet Gatekeeper RCA:
 - (a) receives and authenticates the request;
 - (b) ensures the Certificate and Public Key are current;
 - (c) prioritises the request according to the time of receipt of that request;

- (d) suspends the Certificate;
 - (e) adds the Certificate to its CRL and publishes it to the SecureNet Certificate Repository; and
 - (f) issues a notice containing the Certificate details and the date and time of suspension to the Certificate owner.
3. The suspension of the SecureNet Gatekeeper RCA self-signed Certificate may only be removed:
- (a) after consultation with NOIE;
 - (b) after the SecureNet PMA has met and a resolution has been made to lift the suspension of the SecureNet Gatekeeper RCA's Certificate; and
 - (c) a written authorisation to lift the suspension of the SecureNet Gatekeeper RCA's Certificate has been issued by the SecureNet PMA to the SecureNet Operations Manager.
4. If the SecureNet PMA decides not to lift the suspension of the SecureNet Gatekeeper RCA's Certificate, or the suspension cannot be lifted within the suspension period, revocation of the SecureNet Gatekeeper RCA's Certificate is initiated (see Section 4.4.4, Procedure for revocation request).
5. The SecureNet Gatekeeper RCA verification requirements for Client CA suspension requests are the same as for Certificate re-issuance, and because of these requirements, such requests shall be delivered to the SecureNet Gatekeeper RCA either in the form of digitally signed file, or out-of-band using one of the out-of-band methods provided for in 2.4.2.4.

4.4.9 Limits on suspension period

- 1. The suspension period for the SecureNet Gatekeeper RCA Certificate shall be no longer than one business day.
- 2. The suspension period for a Client CA Certificate shall be no longer than five business days.

3. If the suspension of a Client CA Certificate has not been lifted by the expiration of the 5 day period, the SecureNet Gatekeeper RCA will immediately revoke the Client CA Certificate.

4.4.10 CRL issuance frequency

The CRL in the SecureNet X.500 Directory is updated each time a Certificate that has been issued under this CP is revoked.

4.4.11 CRL checking requirements

Relying Parties must check the validity and currency of a Certificate for every transaction.

4.4.12 On-Line revocation/status checking availability

SecureNet provides an on line mechanism for downloading the CRL from the SecureNet X.500 Directory to verify the status of Certificates issued under this CP.

4.4.13 On Line revocation checking requirements

A Relying Party must check the CRL on a per transaction basis.

4.4.14 Other forms of revocation advertisements available

Because of the significance of the SecureNet Gatekeeper RCA Certificate as the highest point of trust in the SecureNet Gatekeeper PKI Hierarchy, SecureNet shall, in addition to updating the CRL, place a notice on the SecureNet Website in the event that the SecureNet Gatekeeper RCA Certificate is revoked.

4.4.15 Checking requirements for other forms of revocation advertisements

The Relying Party must check the SecureNet Website for any current revocation notices on a per transaction basis.

4.4.16 Special requirements re key compromise

There are no variations to Certificate revocation and suspension procedures when the revocation or suspension is due to CA Private Key compromise.

4.5 Security Audit procedures

Refer to section 4.5 of the SecureNet Gatekeeper CPS.

4.6 Records Archival

Refer to section 4.6 of the SecureNet Gatekeeper CPS.

4.7 Key changeover

1. SecureNet Gatekeeper RCA Key changeovers and Client CA Key changeovers:
 - (a) require, in the case of the SecureNet Gatekeeper RCA, reasonable notice to all Client CAs;
 - (b) must be formally applied for using the application process outlined in Section 4.1, Certificate Application;
 - (c) must be effected in such a manner as to cause minimal disruption to the Client CA's Subscribers; and
 - (d) must be manually effected — no automatic Key changeover processes are supported under the SecureNet Gatekeeper PKI Hierarchy.
2. The SecureNet Gatekeeper RCA and all Client CAs shall each obtain a new Authentication Key Pair a minimum of two years prior to the expiry of the Certificate associated with the current Private Authentication Key, and then commence signing new Certificates with the new Private Authentication Key.
3. During this changeover period until the expiry of the Certificate associated with the current SecureNet Gatekeeper RCA or Client CA Private Authentication Key, both Authentication Public Keys in the associated Certificate will be in use and shall be published in the relevant X.500 Directory.

4.8 Compromise and Disaster Recovery

1. The SecureNet Gatekeeper RCA maintains detailed documentation covering:
 - (a) *SE 03 - Disaster Recovery and Business Continuity Plan*;
 - (b) *AD 01B - Configuration Baseline* of the SecureNet Gatekeeper PKI Hierarchy;
 - (c) *AD 01C - X.500 Object Identifier Tree*; and
 - (d) backup, archiving and offsite storage (in *AD 01 - Certificate Authority Operations Manual*).
2. These plans will be made available to those persons responsible for conducting a security audit.

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

The *AD 01B - Configuration Baseline*, Backup and Archiving in the *AD 01 - Certificate Authority Operations Manual*, and *SE 03 - Disaster Recovery and Business Continuity Plan* shall provide data for identifying component failures, and managing subsequent service restoration.

4.8.2 SecureNet CA Public Key is revoked

SecureNet has established a Key and user compromise plan that addresses the actions to be taken in the event that the SecureNet Gatekeeper RCA Certificate is revoked. This is documented in the *SE 03 - Disaster Recovery and Business Continuity Plan*.

4.8.3 SecureNet CA Private Key is compromised

1. SecureNet has established a Key and user compromise procedure that addresses the actions to be taken in the event that the SecureNet Gatekeeper RCA Private Key is compromised. This procedure is documented in *SE 03 - Disaster Recovery and Business Continuity Plan*.
2. The SecureNet Gatekeeper RCA shall promptly advise NOIE of any compromise or suspected compromise of its Private Keys.

4.8.4 Secure facility after a natural or other type of disaster

Backup, archive and offsite storage are managed in accordance with the *AD 01 - Certification Authority Operations Manual*.

4.8.5 Contingency & Disaster Recovery Plan

The SecureNet Gatekeeper RCA is covered by *SE 03 - Disaster Recovery and Business Continuity Plan* that addresses the actions to be taken in order to restore core business operations as quickly as practicable when system operations have been significantly and adversely impacted by fire, strikes, etc.

4.9 CA termination

4.9.1 Introduction

1. The function of this section is to identify the circumstances in which a termination of all or part of the SecureNet Gatekeeper PKI Hierarchy could occur, and to spell out the rights and obligations of the parties in these circumstances. The function of this section is also to ensure that:
 - (a) the parties co-operate with each other in minimising any disruption that may be caused; and,
 - (b) the parties' capacity to use the SecureNet Gatekeeper PKI Hierarchy is maintained.
2. Full details of the rights and obligations of the various participants will be set out in a business continuity plan (*SE 03 - SecureNet Disaster Recovery and Business Continuity Plan*) and the contracts between relevant participants. For this reason, the full range of circumstances under which it will be necessary to activate the *SE 03 - SecureNet Disaster Recovery and Business Continuity Plan* are not set out in this CP. However, some of the circumstances where activation of the *SE 03 - SecureNet Disaster Recovery and Business Continuity Plan* will be necessary, and the sorts of rights and obligations that will be included, are set out below.

3. The obligations set out in the *SE03 – Disaster Recovery & Business Continuity Plan* (and the relevant contracts) must be undertaken, as relevant, by:
 - (a) the Commonwealth of Australia acting through NOIE; and
 - (b) the Commonwealth Agency receiving the certification products and/or services; and
 - (c) SecureNet; and,
 - (d) any other party who is providing products or services to the Commonwealth Agency for the purposes of implementing Gatekeeper compliant public key technology, whether or not that party has a contractual relationship with SecureNet;

except where a party described at (c) of (d) above has ceased to provide products or services to the Commonwealth Agency for any reason including:

- (e) the expiration of the contract; or
- (f) the relevant contract is to be, or has been, terminated for default or for convenience; or
- (g) one of the parties becomes, or threatens to become, or is in jeopardy of becoming, subject to any form of insolvency administration.

4.9.2 RCA Programmed Termination

1. A programmed termination will arise where there is termination by the SecureNet Gatekeeper RCA for default or for convenience.
2. Insofar as it is required, the SecureNet Gatekeeper RCA shall effect a transfer of its Keys and Certificates to another Gatekeeper Accredited RCA (Replacement RCA) in a manner agreed with NOIE.

3. If programmed termination is required by the SecureNet Gatekeeper RCA, then:
 - (a) The SecureNet Gatekeeper RCA will:
 - (i) give to NOIE and any affected Commonwealth Agencies 3 months' prior written notice of its intention to terminate its RCA operations; and
 - (ii) reasonably co-operate with NOIE and all relevant Commonwealth Agencies in the selection of the Replacement RCA to take over RCA operations; and
 - (iii) transfer the Private Key of the SecureNet Gatekeeper RCA to the Replacement RCA, in a highly secure and trustworthy manner, which manner will be approved by NOIE; and
 - (iv) transfer the CRL and other directories of Certificates issued by the SecureNet Gatekeeper RCA to the Replacement RCA, in a highly secure and trustworthy manner, which manner will be approved by NOIE; and
 - (v) immediately after the transfer of the SecureNet Gatekeeper RCA Private Key to the Replacement RCA, permanently destroy all copies of the SecureNet Gatekeeper RCA Private Key in its possession so that the only copy of the SecureNet Gatekeeper RCA Private Key that is used to digitally sign the SecureNet Gatekeeper RCAs' Public Key Certificates is held by the Replacement RCA; and
 - (vi) provide a formal declaration concerning the destruction of the SecureNet Gatekeeper RCA Private Key (referred to above) to the Competent Authority, other relevant Commonwealth Agencies and relevant Client CAs and RAs; and
 - (vii) use its reasonable endeavours to cause the Replacement RCA within a reasonable time after the date on which the transfer is effected to re-issue new Public Key Certificates for each entity within its PKI Hierarchy that has been transferred; and

- (b) All relevant Commonwealth Agencies will reasonably co-operate with the SecureNet Gatekeeper RCA in the programmed termination of the SecureNet Gatekeeper RCA.

4.9.3 CA Non-programmed Termination

1. A non-programmed termination would arise where, pursuant to a law (State or Commonwealth), it becomes illegal for SecureNet to continue the business operations of the RCA (e.g. SecureNet becomes insolvent).
2. If the SecureNet Gatekeeper RCA is required to implement a non-programmed termination of its business operations, then a representative of the SecureNet Gatekeeper RCA will immediately advise the Competent Authority and the other members of the SecureNet Gatekeeper PKI Hierarchy in writing, or if writing is inappropriate the representative may advise by telephone, that the SecureNet Gatekeeper RCA will be immediately terminating its business operations.
3. In this case:
 - (a) all affected Commonwealth Agencies and other members of the SecureNet Gatekeeper PKI Hierarchy will, with the assistance of the SecureNet Gatekeeper RCA, co-ordinate and use all reasonable endeavours to facilitate the transfer of the CRL and other directories of Certificates issued by the SecureNet Gatekeeper RCA, and the transfer of the SecureNet Gatekeeper RCA's Private Key to a Gatekeeper Accredited replacement RCA (Replacement RCA);
 - (b) The RCA or its administrator/controller/liquidator or representative will:
 - (i) assist to the highest degree possible in the transfer of the Private Key of the SecureNet Gatekeeper RCA to the Replacement CA, in a highly secure and trustworthy manner, which manner will be approved by NOIE; and

- (ii) assist to the highest degree possible in the transfer of the CRL and other directories of Certificates issued by the SecureNet Gatekeeper RCA to the Replacement CA, in a highly secure and trustworthy manner, which manner will be approved by NOIE; and
- (iii) immediately after the transfer of the SecureNet Gatekeeper RCA Private Key to the Replacement CA, permanently destroy all copies of the SecureNet Gatekeeper RCA Private Key in its possession so that the only copy of the SecureNet Gatekeeper RCA Private Key that is used to digitally sign SecureNet Gatekeeper RCA Public Key Certificates is held by the Replacement RCA;
- (iv) provide a formal declaration concerning the destruction of the SecureNet Gatekeeper RCA Private Key (referred to above) to the Competent Authority, relevant Commonwealth Agencies and relevant CAs and RAs;
- (v) use its reasonable endeavours to cause the Replacement CA within a reasonable time after the date on which the transfer is effected to re-issue new Certificates for each entity within the SecureNet Gatekeeper PKI Hierarchy that has been transferred.

4.9.4 Client CA Termination

The processes for termination of a Client CA, both programmed and non-programmed, is fully described in all CPs applicable to Certificates that that Client CA will issue.

4.9.5 Transfer of Root CA Data

The transfer of the Private Key of the SecureNet Gatekeeper RCA and the transfer of Client CA Certificates to a Replacement RCA are dependent upon SecureNet receiving a fair and just price for the transfer.

5. Physical, procedural, and personnel security controls

The SecureNet Gatekeeper RCA CPS provides details of:

- (a) Physical Controls such as:
 - (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; and
 - (viii) Off-site backup.
- (b) Procedural Controls such as:
 - (i) Trusted roles;
 - (ii) The number of persons required per task; and
 - (iii) Identification and authentication for each role.
- (c) Personnel Controls such as:
 - (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; and
- (viii) Documentation supplied to personnel.

6. Technical Security Controls

6.1 Key Pair Generation

6.1.1 Key pair generation

1. SecureNet Gatekeeper RCA Key pairs are generated and installed by the SecureNet Gatekeeper RCA using software that is listed on the EPL.
2. Client CA Key pairs are generated by the Client CA itself using software, equipment and processes which meet Gatekeeper requirements.

6.1.2 Private Key delivery to entity

1. The self-generated SecureNet Gatekeeper RCA Private Keys do not require delivery.
2. Client CA Private Keys are generated by the Client CA and do not require delivery.

6.1.3 Public Key delivery to Certificate issuer

1. The self-generated SecureNet Gatekeeper RCA Public Keys do not require delivery.
2. Client CA Public Keys are delivered to the SecureNet Gatekeeper RCA in the form of a PKCS#10 Certificate request file, personally escorted by trusted Client CA personnel.

6.1.4 CA Public Key delivery to users

1. The self-generated SecureNet Gatekeeper RCA Public Key Certificates are published in the SecureNet X.500 Directory, and copies are provided to Client CAs as part of the response process for Client CA Certification Requests.
2. Client CA Certificates are published by the SecureNet Gatekeeper RCA in the SecureNet X.500 Directory.

6.1.5 Key sizes

1. The SecureNet Gatekeeper RCA Key length is 2048 bits.
2. Client CA key lengths are at least 1024 bits.

6.1.6 Public Key parameters generation

1. The parameters used to create the SecureNet Gatekeeper RCA Public Keys are generated by the SecureNet Gatekeeper RCA.
2. The parameters used to create the Client CA Public Keys are generated by the Client CA.
3. In both cases, the generation of Public Key parameters has been certified in the course of ITSEC E3 evaluation of the CA products used for Key generation.

6.1.7 Parameter quality checking

1. Parameter quality checking (including primality testing for prime numbers where appropriate) has been certified in the course of ITSEC E3 evaluation of the CA products used for SecureNet Gatekeeper RCA Key generation.
2. Parameter quality checking (including primality testing for prime numbers where appropriate) shall have been certified in the course of ITSEC E3 evaluation of the CA products used for Client CA Key generation.

6.1.8 Hardware/software Key generation

1. SecureNet Gatekeeper RCA Key generation is performed using software that is listed on the EPL.
2. Client CA Key generation shall be performed using products that are listed on the EPL.

6.1.9 Key usage purposes

1. SecureNet Gatekeeper RCA Keys will be used for the purposes and in the manner described in Section 1.3.6.1 of this CP.

2. Client CA Keys shall be used for the purposes and in the manner described in the Client CA CP. Any restrictions described in the CP shall be observed.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

1. Cryptographic modules are not used by the SecureNet Gatekeeper RCA.
2. Where cryptographic modules are used by Client CAs, they shall be evaluated to ITSEC E3 standards, and shall be listed on the EPL.

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

1. SecureNet Gatekeeper RCA Private Keys are not under n out of m multi-person control.
2. At least dual person control shall be present for all operations concerning Client CA or SecureNet Gatekeeper RCA Private Keys

6.2.3 Private Key escrow

1. Private Key escrow is not supported or permitted by the SecureNet Gatekeeper RCA.
2. Private Key escrow by a third party shall not be supported or permitted by Client CAs.

6.2.4 Private Key backup

1. The SecureNet Gatekeeper RCA Private Key is stored in an encrypted file, which is backed up, with backup copies maintained on site and in secure off site storage.
2. Backup of a Client CA Private Key shall be specified in the Client CA CP.

6.2.5 Private Key archival

1. For the SecureNet Gatekeeper RCA, see Section 4.6 of the SecureNet Gatekeeper CPS.

2. Archival arrangements for a Client CA Private Key shall be specified in the Client CA CP.

6.2.6 Private Key entry into cryptographic module

1. Cryptographic modules are not used by the SecureNet Gatekeeper RCA.
2. Where cryptographic modules are used by a Client CA, the Client CA Key Management Plan shall specify who enters the Private Key into the cryptographic module, and in what form the Private Key is entered and stored in the module.

6.2.7 Method of activating Private Key

1. The SecureNet Gatekeeper RCA Private Keys are activated by the SecureNet Gatekeeper RCA software, following the successful completion of a login process that requests and validates an authorised user access control mechanism.
2. The Client CA Key Management Plan shall specify who can activate or use Private Keys and how entity authentication is required to activate the Private Key. Entry of Activation Data shall be protected from disclosure (i.e. the data should not be displayed while it is entered).

6.2.8 Method of deactivating Private Key

1. SecureNet Gatekeeper RCA Private Keys are de-activated when the SecureNet Gatekeeper RCA software application is terminated.
2. The Client CA Key Management Plan shall specify who can deactivate Private Keys and how.

6.2.9 Method of destroying Private Key

1. The SecureNet Gatekeeper RCA software destroys Private Keys in memory when the software shuts down.
2. The Client CA Key Management Plan shall specify who can destroy Private Keys and how.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key archival

1. The SecureNet Gatekeeper RCA archives all Certificates it generates, including the SecureNet Gatekeeper RCA self-signed Certificate.
2. Each Client CA will archive a copy of its Client CA Certificate.

6.3.2 Usage periods for the Public Keys and Private Keys

1. The SecureNet Gatekeeper RCA Key Pairs have the following usage periods:
 - (a) Authentication Private and Public Keys – 20 years;
 - (b) Confidentiality Public Key – 20 years;
 - (c) Confidentiality Private Key – no expiry.
2. Usage periods for Client CA public and private keys shall be specified in the Client CA CP.

6.4 Activation Data

6.4.1 Activation data generation and installation

1. No activation data other than dual control access mechanisms is required to operate the SecureNet Gatekeeper RCA software.
2. Activation Data together with any other access control mechanisms used by Client CAs should have the level of strength appropriate to the Keys or data to be protected.

6.4.2 Activation data protection

1. No activation data other than dual control access mechanisms is required to operate the SecureNet Gatekeeper RCA software, which is housed in a Highly Protected physical environment.
2. Data used to activate Client CA Private Keys shall be protected from disclosure by at least a combination of procedural and physical access control mechanisms.

6.4.3 Other aspects of activation data

No Stipulation.

6.5 Computer Security Controls

The SecureNet Gatekeeper CPS provides details of:

- (a) specific computer security technical requirements; and
- (b) computer security rating;

relevant to the operation of the SecureNet Gatekeeper PKI Hierarchy.

6.6 Life Cycle Technical Controls

The SecureNet Gatekeeper CPS provides details of:

- (a) System development controls;
- (b) Security management controls; and
- (c) Life cycle security ratings;

relevant to the operation of the SecureNet Gatekeeper PKI Hierarchy.

6.7 Network security controls

Refer section 6.7 of the SecureNet Gatekeeper CPS.

6.8 Cryptographic module engineering controls

Cryptographic modules are not used by the SecureNet Gatekeeper RCA.

7. Certificate and CRL Profiles

7.1 CA Certificate Profiles

7.1.1 Version number(s)

1. The SecureNet Gatekeeper RCA supports the use of X.509 Version 3 Certificates.
2. Certificates issued by the SecureNet Gatekeeper RCA include the following fields:
 - (a) the version field, populated with an integer value of 2 to indicate that the Certificate is a version 3 Certificate;
 - (b) the serial number field, populated with a unique positive integer value to indicate the Certificate's serial number for each CA;
 - (c) the issuer field, populated with the X.500 distinguished name of the SecureNet Gatekeeper RCA;
 - (d) the validity field, populated with the time period for which the Certificate is considered valid (with both 'Not Before' and 'Not After' dates encoded as UTCTime for dates up to 2049, and encoded as GeneralizedTime for dates in 2050 or later); and
 - (e) the subject field, populated with the X.500 distinguished name of the subject to whom the Certificate was issued i.e. the SecureNet Gatekeeper RCA or Client CA, as applicable.
3. Client CAs shall support the use of X.509 Version 3 Certificates.

7.1.2 Certificate extensions

1. The SecureNet Gatekeeper RCA supports the use of X.509 Version 3 Certificate extensions and uses the following standard extensions within the SecureNet Gatekeeper RCA Certificate:
 - (a) NetscapeCertType (flagged non-critical);

- (b) Certificate Policies (flagged non-critical);
 - (c) Basic Constraints (flagged critical).
2. Certificate extensions required in Client CA Certificates issued by the SecureNet Gatekeeper RCA must be specified in the Client CA's Certificate application.
 3. Client CAs shall support the use of X.509 Version 3 Certificate extensions.

7.1.3 Algorithm object identifiers

1. SecureNet OIDs are not allocated to algorithms supported and used within the SecureNet Gatekeeper PKI Hierarchy. Only published Algorithm OIDs are used.
2. The following hashing/digest algorithms are supported in SecureNet PKI Hierarchies:
 - (a) Secure Hash Algorithm-1;
 - (b) Message Digest 5 (MD5).
3. The following padding algorithms are supported in SecureNet PKI Hierarchies:
 - (a) ISO 9796;
 - (b) PKCS#1.
4. The following encryption algorithms are supported in SecureNet PKI Hierarchies:
 - (a) RSA;
 - (b) DES.
5. The following authentication algorithms are supported in SecureNet PKI Hierarchies:
 - (a) RSA;
 - (b) DSA.

6. The use of multiple algorithms within the same hierarchy is supported.

7.1.4 Name forms

Certificates issued by the SecureNet Gatekeeper RCA contain the full X.500 distinguished name of the Certificate issuer and Certificate subject in the issuer name and subject name fields respectively.

7.1.5 Name constraints

Anonymous names are not supported by the SecureNet Gatekeeper RCA. Pseudonymous names that may cause offence are not permitted.

7.1.6 Certificate policy Object Identifier

The OID of this CP is carried in the standard extension field of issued X.509 Certificates and is published in Section 1.2.2, SecureNet Gatekeeper RCA CP OID.

7.1.7 Usage of Policy Constraints extension

The SecureNet Gatekeeper RCA supports the use of the Policy Constraints extension.

7.1.8 Policy qualifiers syntax and semantics

The SecureNet Gatekeeper RCA supports the use of syntax and semantics policy qualifiers.

7.1.9 Processing semantics for the critical Certificate policy extension

See Section 7.1.2, Certificate extensions.

7.2 CRL Profile

7.2.1 Version number(s)

1. The SecureNet Gatekeeper RCA supports the use of X.509 Version 2 CRLs.
2. Client CAs shall support the use of X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

1. The SecureNet Gatekeeper RCA supports the use of X.509 Version 2 CRL entry extensions.
2. Client CAs shall support the use of X.509 Version 2 CRL entry extensions.

8. Specification Administration

1. SecureNet operates a PMA which has the responsibility for setting Certificate policy direction for the overall SecureNet Gatekeeper PKI. Contact details for the SecureNet PMA are given in Section 1.3.1.2.1, SecureNet PMA Contact details.
2. Each CP relevant to the SecureNet Gatekeeper PKI Hierarchy has been allocated an OID. The OID provides a unique identifier for each CP which includes a policy version number. Details of the OID for this CP may be found in Section 1.2.2, SecureNet Gatekeeper RCA CP OID.

8.1 Specification change procedures

8.1.1 Initial publication

1. The initial publication of this CP occurs once it has been approved by the Competent Authority.
2. The responsible authority for changes to this CP is the SecureNet PMA. The SecureNet Gatekeeper RCA has received formal endorsement and been allocated an OID by the SecureNet PMA.
3. The SecureNet PMA is responsible for:
 - (a) advising all subordinate entities of the SecureNet Gatekeeper RCA CP and its applicability;
 - (b) forwarding a copy of the SecureNet Gatekeeper RCA CP to each Client CA along with an advice about where the CP can be read; and
 - (c) advising each Client CA of any changes made to this CP.

8.1.2 Change

1. Changes to this CP must be approved by the Competent Authority.

2. Two forms of policy change are contemplated:
 - (a) issue of a new SecureNet Gatekeeper RCA CP; and
 - (b) change or alteration of the existing SecureNet Gatekeeper RCA CP.
3. Where a change to the SecureNet Gatekeeper RCA CP is required, the OID of the policy will remain in force, however a new version number will be allocated by the PMA on endorsement of the SecureNet Gatekeeper RCA CP by the SecureNet PMA.
4. Following approval, the SecureNet PMA will facilitate publication of the new SecureNet Gatekeeper RCA CP.
5. Any changes to this CP must be made in accordance with the Gatekeeper Accreditation requirements.

8.2 Publication and notification policies

1. The new or changed SecureNet Gatekeeper RCA CP will be published on the SecureNet Website.
2. All Client CAs will be notified by the SecureNet PMA of any changes to this CP at least one week prior to its publication.

8.3 CP approval procedures

New or updated versions of this CP must be endorsed by the SecureNet PMA, certified by an Authorised Evaluator and approved by the Competent Authority to maintain its Gatekeeper Accredited status.

9. APPENDIX A

CERTIFICATE APPLICATION

Certificate Service Required (Choose one from each group)

New Certificate Certificate Renewal

Applicant Organisation Information

Organisation Name: _____ ABN: _____

Phone: _____ Facsimile: _____

Street Address: _____

Suburb: _____ State: _____ Postcode: _____

Postal Address: _____

Suburb: _____ State: _____ Postcode: _____

Type of Organisation: Government Agency Company Other _____

Client CA Certificate Characteristics

Preferred Certificate Name (Choose one)

Organisation Name Trademark Trademark details: _____

Required Extensions: pathLenConstraint: Required value:

policyMappings:

IssuerDomainPolicy: _____ subjectDomainPolicy: _____

nameConstraints: (if more room required, document separately and attach)

permittedSubtrees: _____

Other (if more room required, document separately and attach) _____

Organisation Officer Information

Surname: _____ Given Names: _____

Position Held: _____ Work Phone: _____

Mobile Phone: _____ After Hours Phone: _____ Fax: _____

Email Address: _____ DOB: _____

Shared secret: _____ (eg: Mother's Maiden Name)

Applicant Agreement

I certify (a) that the above particulars are correct, (b) that I am the Organisation Officer described above, (c) that the Organisation's CA has been granted Full Gatekeeper Accreditation by the Competent Authority, and (d) that I am authorised to execute and deliver this application on behalf of the Organisation. In signing this application for a Client CA digital Certificate, I confirm that the Organisation and I agree to adhere to the responsibilities and obligations defined in the Certificate Policy under which the Certificate I have applied for is issued and the SecureNet Gatekeeper Certification Practice Statement (CPS), which outline the conditions of use and acceptance of a Certificate, and I agree on behalf of myself and my Organisation to be bound by those documents, and any SecureNet-Client CA Agreement. In particular, I will make appropriate arrangements to protect the Client CA's private key(s), Attached to this application are:

proof of Full Gatekeeper Accreditation **OR** proof of Full Gatekeeper Accreditation already provided.

Organisation Officer Signature: _____ Date: _____

Witness: _____ **Signature:** _____ **Date:** _____
(name – print)

10. APPENDIX B

CERTIFICATE SUSPENSION/UNSUSPENSION REQUEST

Date:

To: SecureNet Root Certification Authority
Trust Centre, 15 Whiting Street, Artarmon NSW 2067

Section 1 – Certificate details (if known)

Certificate ID: _____

Certificate serial number: _____

Section 2 – Request Details

Suspension

Unsuspension

Section 3 – Certificate Owner/Requestor Details

CLIENT CA:

Organisation: _____

Organisation Officer:

Full name: _____
(Given names) (Surname)

Department: _____

Position in organisation: _____

Contact phone number: _____

(Requestor must be available on this number to confirm request)

Section 3 – Reason for Suspension/Unsuspension *

* Optional for Certificate holders requesting Suspension of their own Certificates

Section 4 – Authorisation

Authorised by: Organisation Officer of Client CA

SecureNet PMA

Authorised third party

(Original documentation verifying authorisation must be sighted.)

Signature: _____

11. APPENDIX C

CERTIFICATE REVOCATION REQUEST

Date: _____

To: SecureNet Root Certification Authority
Trust Centre, 15 Whiting Street, Artarmon NSW 2067

Section 1 – Certificate details (if known)

Certificate ID: _____

Certificate serial number: _____

Section 2 – Certificate Owner/Requestor Details

Client CA:

Organisation: _____

Organisation Officer:

Full name: _____

(Given names)

(Surname)

Department: _____

Position in organisation: _____

Contact phone number: _____

(Requestor must be available on this number to confirm request)

Section 3 – Reason for Revocation *

* Optional for Certificate holders requesting Suspension of their own Certificates

Section 4 – Authorisation

Authorised by: Organisation Officer of Client CA

SecureNet PMA

Authorised third party

PO 01 - SecureNet RCA-Issued Certificates Policy — Version 0.9A

(Original documentation verifying authorisation must be sighted.)

Signature: _____