



Baltimore Certificates On-Line

CAPL – 006 (CP – ST) Certificate Practice
Statement

Serial Number	
Release	Version 1.5
Status	Final
Issue Date	02 May 2000

Copyright © 2000 Certificates Australia Proprietary Limited,
ACN 075878867

All Rights Reserved

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 Certificates Australia Proprietary Limited.

Table of Contents

Table of Contents.....	1
CERTIFICATE PRACTICE STATEMENT	1
1. INTRODUCTION.....	2
1.1 Overview.....	2
1.1.1 Standards.....	3
1.1.2 Certificate types issued	3
1.1.3 Definitions	5
1.1.4 X500 Object Identifier hierarchy.....	5
1.1.5 Certificate Management Life Cycle.....	6
1.1.6 PKI Operational Infrastructure.....	11
1.1.7 Scope	13
1.1.8 Security Philosophy	14
1.1.9 Staffing Arrangements	14
1.1.10 Right of Inquiry.....	15
1.2 Identification.....	15
1.3 Community and Applicability	15
1.3.0 Policy Authorities	16
1.3.1 Certification authorities	17
1.3.2 Registration Authorities.....	21
1.3.3 End Entities.....	23
1.3.4 Applicability.....	23
1.4 Contact Details	27
1.4.1 Specification administration organisation	27
1.4.2 Contact person	27
1.4.3 Person determining CPS suitability for this policy.....	28
2. GENERAL PROVISIONS.....	29
2.1 Obligations	29
2.1.0 CAPL Obligations.....	29
2.1.1 CA Obligations.....	31
2.1.2 RA Obligations.....	32
2.1.3 Subscriber Obligations.....	33
2.1.4 Relying party obligations	34
2.1.5 Repository Obligations.....	35
2.2 Liability.....	35
2.2.0 CAPL Liability.....	35
2.2.1 CA Liability.....	36
2.2.2 RA Liability.....	36
2.2.3 End Entity Liability	36

2.3	Financial responsibility.....	36
2.3.1	Indemnification by relying parties	36
2.3.2	Fiduciary relationships	36
2.3.3	Administrative processes	36
2.3.4	Certificates Australia Pty Limited.....	36
2.3.5	Client managed CA and RA services	36
2.4	Interpretation and Enforcement	37
2.4.1	Governing Law	37
2.4.2	Severability, survival, merger, notice.....	37
2.4.3	Dispute resolution procedures	38
2.5	Fees	38
2.5.1	Certificate issuance or renewal fees	38
2.5.2	Certificate access fees	38
2.5.3	Revocation or status information access fees.....	38
2.5.4	Fees for other services such as policy information.....	38
2.5.5	Refund policy.....	38
2.6	Publication and repository	38
2.6.1	Publication of CA information.....	38
2.6.2	Frequency of publication	39
2.6.3	Access controls.....	39
2.6.4	Repositories	40
2.7	Compliance Audit.....	42
2.7.0	GPKA Evaluation	42
2.7.1	Frequency of entity compliance audit.....	42
2.7.2	Identity/qualifications of auditor.....	43
2.7.3	Auditor's relationship to audited party.....	43
2.7.4	Topics covered by audit	43
2.7.5	Actions taken as a result of deficiency	44
2.7.6	Communication of results.....	44
2.8	Confidentiality and privacy	44
2.8.1	Types of information to be protected.....	44
2.8.2.	Types of information that may be disclosed	46
2.8.3.	Disclosure of Certificate revocation/suspension information	46
2.8.4.	Release to law enforcement officials.....	47
2.8.5.	Release as part of civil discovery	47
2.8.6.	Disclosure upon owner's request	47
2.8.7.	Other information release circumstances	47
2.9	Intellectual Property rights.....	48
2.9.1	General provision.....	48
2.9.2	Copyright.....	48
3.	IDENTIFICATION AND AUTHENTICATION	49
3.0	General	49
3.0.1	CA and RA initial registration.....	49
3.0.2	End Entity initial registration.....	51
3.1	Initial registration	54
3.1.1	Types of names	54

3.1.2	Need for names to be meaningful.....	55
3.1.3	Rules for interpreting various name forms.....	55
3.1.4	Uniqueness of names	55
3.1.5	Name claim dispute resolution procedure	55
3.1.6	Recognition, authentication and role of trademarks.....	55
3.1.7	Method to prove possession of Private Key	55
3.1.8	Authentication of organisation identity	56
3.1.9	Authentication of individual identity.....	56
3.2	Routine Rekey	57
3.3	Rekey after Revocation	57
3.4	Revocation request.....	57
4.	OPERATIONAL REQUIREMENTS.....	59
4.1	Certificate Application	59
4.2	Certificate Issuance.....	59
4.2.1	Certificate issue process.....	59
4.3	Certificate Acceptance.....	61
4.4	Certificate Suspension and Revocation	62
4.4.1	Circumstances for revocation.....	62
4.4.2	Who can request revocation	63
4.4.3	Procedure for revocation request.....	64
4.4.4	Revocation request grace period	66
4.4.5	Circumstances for suspension.....	66
4.4.6	Who can request suspension	66
4.4.7	Procedure for suspension request.....	67
4.4.8	Limits on suspension period.....	67
4.4.9	CRL issuance frequency	67
4.4.10	CRL checking requirements	67
4.4.11	On-Line revocation/status checking availability	67
4.4.12	On-Line revocation checking requirements	67
4.4.13	Other forms of revocation advertisements available	67
4.4.14	Checking requirements for other forms of revocation advertisements.....	67
4.4.15	Special requirements re key compromise.....	68
4.5	Security Audit procedures	68
4.5.1	Types of event recorded	68
4.5.2	Frequency of processing log.....	68
4.5.3	Retention period for audit log	68
4.5.4	Protection of audit log.....	69
4.5.5	Audit log backup procedures	69
4.5.6	Audit collection system	69
4.5.7	Notification to event-causing subject	69
4.5.8	Vulnerability assessments	70
4.6	Records Archival	70
4.6.1	Types of event recorded	70
4.6.2	Retention period for archive	70
4.6.3	Protection of archive	71

4.6.4	Archive backup procedures	71
4.6.5	Requirements for time-stamping of records	71
4.6.6	Archive collection system	71
4.6.7	Procedures to obtain and verify archive information	71
4.7	Key changeover.....	71
4.8	Compromise and Disaster Recovery	72
4.8.1	Computing resources, software, and/or data are corrupted	72
4.8.2	Entity Public Key is revoked.....	73
4.8.3	Entity Private Key is compromised	73
4.8.4	Secure facility after a natural or other type of disaster	73
4.8.5	Contingency & Disaster Recovery Plan	73
4.9	CA Termination	74
4.9.1	Introduction.....	74
4.9.2.	CAPL RCA Programmed Termination.....	75
4.9.3.	CAPL RCA Non-programmed Termination.....	76
4.9.4.	Non-Commonwealth CA Business Operations Programmed Termination	76
4.9.5.	Non-Commonwealth CA Business Operations Non-programmed Termination	77
4.9.6.	Non-Commonwealth RA business operations Programmed Termination.....	78
4.9.7.	Non-Commonwealth RA business operations Non-programmed Termination	78
5.	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	80
5.1	Physical Controls	80
5.1.1	Site location and construction	80
5.1.2	Physical access	80
5.1.3	Power and air conditioning	80
5.1.4	Water exposures.....	80
5.1.5	Fire prevention and protection.....	80
5.1.6	Media storage.....	80
5.1.7	Waste disposal.....	81
5.1.8	Off-site backup.....	81
5.2	Procedural Controls	81
5.2.1	Trusted roles.....	81
5.2.2	Number of persons required per task.....	81
5.2.3	Identification and authentication for each role	82
5.3	Personnel Controls	82
5.3.1	Background, qualifications, experience, and clearance requirements.....	82
5.3.2	Background check procedures	82
5.3.3	Training requirements	82
5.3.4	Retraining frequency and requirements.....	82
5.3.5	Job rotation frequency and sequence	83
5.3.6	Sanctions for unauthorised actions	83
5.3.7	Contracting personnel requirements	83
5.3.8	Documentation supplied to personnel.....	83
6.	TECHNICAL SECURITY CONTROLS	84
6.1	Key Pair Generation and Installation.....	84
6.1.1	Key pair generation	84

6.1.2	Private Key delivery to entity	84
6.1.3	Public Key delivery to Certificate issuer.....	84
6.1.4	CA Public Key delivery to users.....	84
6.1.5	Key sizes.....	84
6.1.6	Public Key parameters generation	84
6.1.7	Parameter quality checking.....	84
6.1.8	Hardware/software key generation.....	84
6.1.9	Key usage purposes.....	84
6.2	Private Key Protection	85
6.2.1	Standards for cryptographic module	85
6.2.2	Private Key (n out of m) multi-person control.....	85
6.2.3	Private Key escrow.....	85
6.2.4	Private Key backup	85
6.2.5	Private Key archival	85
6.2.6	Private Key entry into cryptographic module	85
6.2.7	Method of activating Private Key	85
6.2.8	Method of deactivating Private Key.....	85
6.2.9	Method of destroying Private Key.....	85
6.3	Other Aspects of Key Pair Management.....	85
6.3.1	Public Key archival.....	85
6.3.2	Usage periods for the public and Private Keys.....	86
6.4	Activation Data.....	86
6.4.1	Activation data generation and installation	86
6.4.2	Activation data protection.....	86
6.4.3	Other aspects of activation data.....	86
6.5	Computer Security Controls.....	86
6.5.1	Specific computer security technical requirements	86
6.5.2	Computer security rating.....	86
6.6	Life Cycle Technical Controls.....	86
6.6.1	System development controls.....	86
6.6.2	Security management controls	86
6.6.3	Life cycle security ratings	86
6.7	Network Security Controls.....	87
6.8	Cryptographic Module Engineering Controls	87
7.	CERTIFICATE AND CRL PROFILES	88
7.1	Certificate Profile	88
7.1.1	Version number(s).....	88
7.1.2	Certificate extensions	88
7.1.3	Algorithm object identifiers	88
7.1.4	Name forms.....	88
7.1.5	Name constraints.....	88
7.1.6	Certificate policy Object Identifier.....	88
7.1.7	Usage of Policy Constraints extension	89
7.1.8	Policy qualifiers syntax and semantics.....	89
7.1.9	Processing semantics for the critical Certificate policy extension.....	89

7.2	CRL Profile	89
7.2.1	Version number(s).....	89
7.2.2	CRL and CRL entry extensions.....	89
8.	SPECIFICATION ADMINISTRATION	90
8.1	Specification change procedures.....	90
8.1.1	Change	90
8.2	Publication and notification policies	91
8.3	CPS approval procedures	91
	Appendix A – CP Supported under this CPS	92

CERTIFICATE PRACTICE STATEMENT

CERTIFICATES AUSTRALIA PTY LIMITED

CERTIFICATE PRACTICE
STATEMENT

ACCREDITATION	Gatekeeper
TYPE:	FULL
GRADE:	Not applicable
VERSION No:	Version 1.5
STATUS:	Final

1. INTRODUCTION

1.1 Overview

This Certificate Practice Statement (CPS) is written expressly for use within the Certificates Australia Pty Limited (CAPL) Public Key Infrastructure (PKI). The CAPL PKI is designed and is operated to comply with the Australian Commonwealth Government's Gatekeeper strategy for the use of Public Key Technology in government.

The CAPL PKI supports the creation and use of key pairs and of Public Key Certificates. Key pairs and Public Key Certificates are used in the provision of CAPL's PKI Certificate services, including but not limited to:

1. authentication services (authentication, integrity and non-repudiation); and,
2. confidentiality services.

This CPS provides factual information that describes the:

1. practices employed within the CAPL PKI to support Certificate services;
2. attendant use of technologies and processes to support the underlying operational infrastructure.

The practices described in this CPS together with the technologies and processes referred to in other specific operational documentation serve to illustrate the trustworthiness and integrity of CAPL's Certificate operations from Certificate generation and signing to expiry.

A number of CPS may be operated under the CAPL PKI, depending on the commercial arrangements in place between CAPL and a Customer and the nature and number of the separate legal entities involved. Each CP will always be associated with a specified CPS.

1.1.0.1 CAPL PKI Certificate Services

CAPL's Certificate services provide a range of security and assurance levels to support various Gatekeeper compliant and GPKA accredited commercial transactions.

The Certificates and associated CP supported under this CPS range from contractual or signatory functions, through to high value financial arrangements such as purchase orders.

Certificates and associated supporting CP are also supportive of the use of either:

1. Non National Security Classification; or,
2. National Security Classification markings.

1.1.0.2 Revisions

This CPS undergoes a regular review process as prescribed by the CAPL Policy Approval Authority (PAA). Revisions of this document are identified through a configuration baseline schema and numbering convention.

1.1.1 Standards

This CPS is referred to as the “Certificates Australia CPS”.

The structure of this CPS is based on the 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 more information see Section 1.1.1 *Standards* in a relevant CP.

This CPS differs from the RFC 2527 standard only to the degree necessary to adequately describe the operational practices used within the CAPL PKI.

1.1.2 Certificate types issued

This CPS supports the operation of:

1. nominated Gatekeeper compliant and GPKA accredited Certificates and supporting CP;
2. nominated ICA Certificates issued by the CAPL RCA;
3. nominated OCA Certificates issued by a CAPL ICA;
4. nominated OCA Certificates issued by a CAPL RCA;
5. nominated RA Certificates issued by CAPL CAs;
6. such other Certificates and supporting CP as may be approved by the CAPL PAA.

CP supported by this CPS are listed in Appendix B – *CP Supported under this CPS* and are published on the web sites at:

www.certificates-australia.com.au

www.secdom.com.au

1.1.2.1 X.509 Certificate extensions

CAPL complies with the X.509 Version 3 standard. Part of this standard defines Certificate extensions that may be used to restrict the use of or convey additional information about a Certificate.

Certificate extensions consist of three fields:

1. type this field indicates the type of data in the value field;

2. criticality this indicates the importance of the information contained in the value field;
3. value this field contains the additional Certificate information.

The CAPL PKI supports Certificate extensions to provide additional information about a Certificate, as prescribed within a relevant CP.

CAPL will maintain a list of certificate extension Object Identifiers used within its infrastructure.

1.1.2.2 Policy qualifier extension

CAPL PKI Certificates use Policy Qualifier extensions. Policy Qualifiers operate to convey important information for the attention of the Certificate owner or a relying party, including information such as:

1. liability; or,
2. information about the signing authority.

1.1.2.3 Approved Policy Qualifiers

CAPL will publish on its web site, Policy Qualifiers that have been approved for use within the hierarchy. Policy Qualifiers will not be inconsistent with its appropriate CP.

1.1.2.4 Other Certificate extensions

Certificates may be issued containing private or service-oriented extensions. Communities of interest may define these extensions to carry information unique to those communities, for example to include additional attributes in an Attribute Certificate.

1.1.2.5 Criticality of Certificate extensions

Certificate extensions are assigned a criticality value of “true” or “false” during Certificate issuance.

Where the criticality of an extension is:

1. “true”, it is the responsibility of relying parties to understand the purpose of the extension and to be aware of any specific processing requirements, otherwise they should place no reliance on the Certificate;
2. “false”, the relying party must make their own determination of the importance of the information and of the need to be aware of any specific processing requirements.

Key Usage fields in all Certificates issued within the CAPL PKI have a criticality value of “true”.

The purpose and meaning of Certificate extensions is explained in the associated CP.

1.1.3 Definitions

This CPS assumes that the reader is familiar with basic PKI concepts, including:

1. the use of digital signatures for authentication, integrity and non-repudiation;
2. the use of encryption for confidentiality;
3. the principles of asymmetric encryption, Public Key Certificates and key pairs;
4. the role of Certification Authorities and Registration Authorities.

Readers wishing further information about PKI should refer to the web sites at:

www.certificates-australia.com.au

www.secdom.com.au

Definitions used within this document are contained in Appendix A – Glossary. These definitions are based on:

1. ISO Glossary of IT Security Technology¹; and,
2. GPKA Glossary of Terms².

The definitions differ from these glossaries only in so far as it is necessary for clarity within the framework of the CAPL PKI hierarchy.

1.1.4 X500 Object Identifier hierarchy

Object Identifiers (OID) have been assigned by CAPL and documented in a Configuration baseline document for X.500 OID Schema.

OIDs are assigned to:

1. the CAPL RCA;
2. each ICA, OCA and CP within the CAPL PKI;
3. Where required, certificate extensions.

OIDs are not assigned to RAs, or to this CPS.

All OID are be recorded in:

1. an appropriate CP:
 - the CAPL RCA OID is recorded in each CP issued under its hierarchy;

¹ Glossary of IT security terminology prepared by JTC1 SC 27 at <http://www.iso.ch:8080/jtc1/sc27/27sd698a.htm>

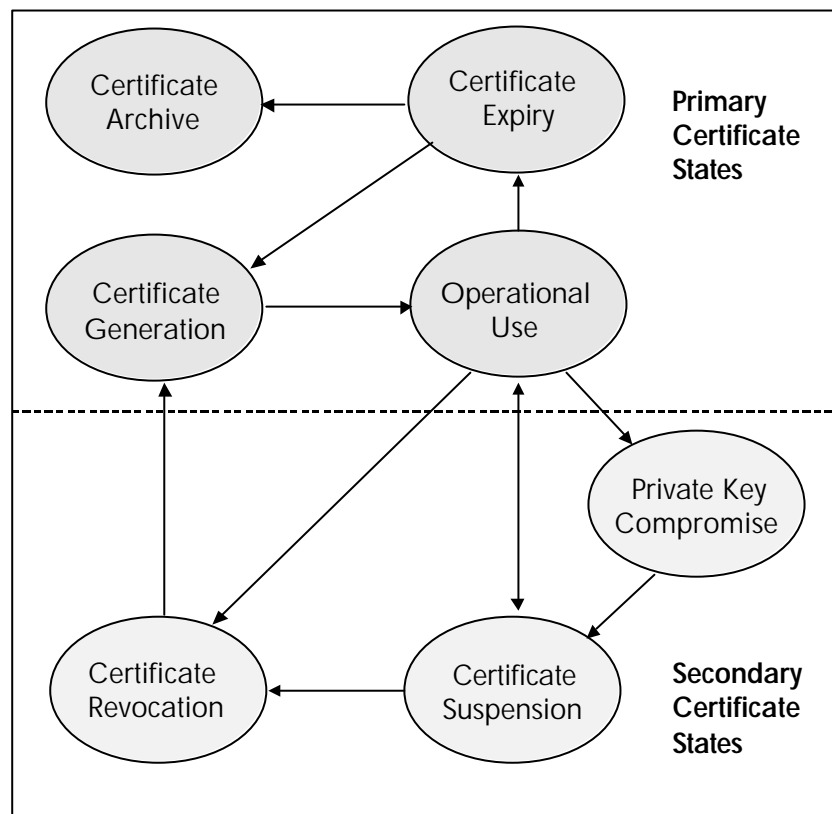
² Government Public Key Authority web site at <http://www.gpka.gov.au/>

- each CA's OID is recorded in each CP under which it issues Certificates;
 - each CP OID is recorded in the relevant CP;
2. internal CAPL records.

1.1.5 Certificate Management Life Cycle

The CAPL Certificate Management Life Cycle (CMLC) is illustrated in Figure 1.1 below. The CMLC applies to all Certificates issued within the CAPL PKI.

Figure 1.1 Certificate Management Life Cycle



The CMLC represents the high-level Certificate management process within the CAPL PKI. It consists of primary and secondary Certificate states. The primary states are:

1. generation;
2. operational use;
3. expiry; and
4. archive

All Certificate types issued pass through these three primary states as part of their life cycle.

The secondary states are:

1. compromise;
2. suspension; and,
3. revocation.

Because these secondary states represent exception situations, it is expected that:

1. most End Entity Certificates will pass through only the primary states during their life cycle;
2. a small number of End Entity Certificates may pass through one or more of the secondary states.

The CAPL PKI supports the CMLC Certificate states in the delivery of all of its Certificates. It should be noted that some Certificate states may be supported on a procedural basis only.

The CMLC does not support a provisional Certificate state. Certificates are issued after a Certificate application has been submitted and approved, and are deemed to be in operational use in accordance with the CP.

A complete copy of the CMLC applicable to CAPL CA service provider may be found at:

www.certificates-australia.com.au

www.secdom.com.au

1.1.5.1. Key Pairs

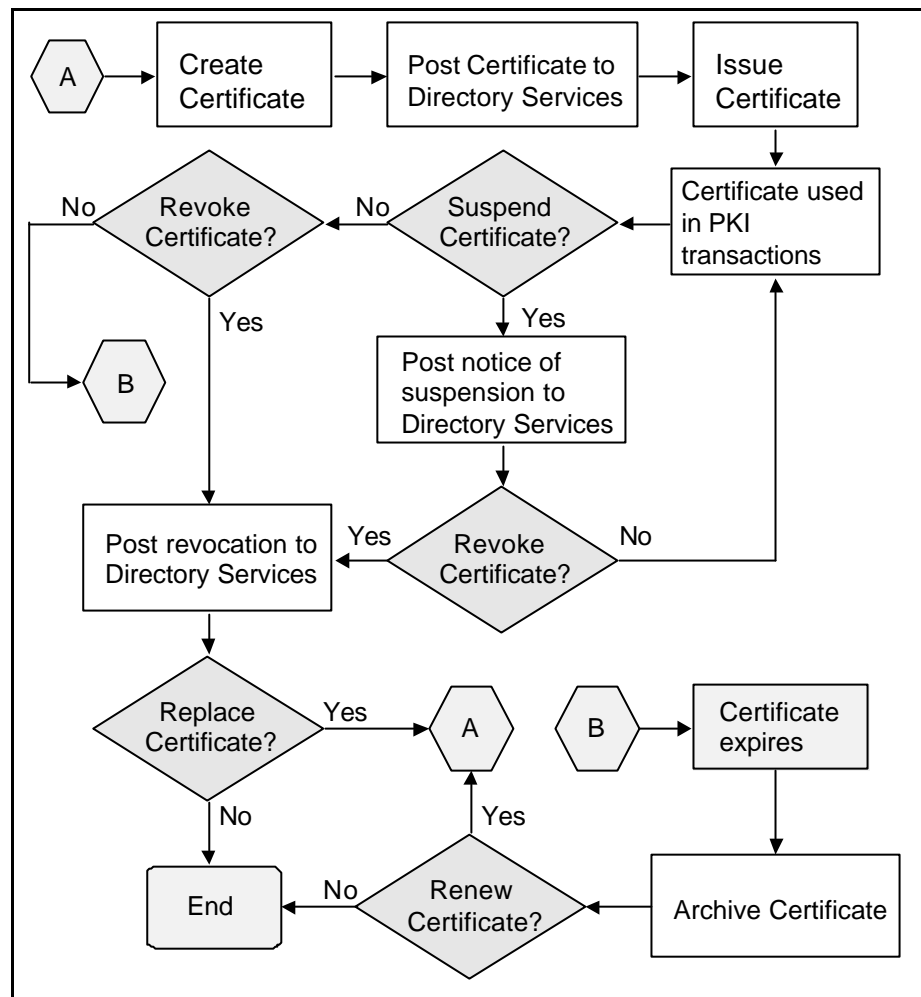
Key pairs are bound to Certificates and are programmed to expire at the same time that the Certificate expires. Key pairs can be registered under more than one Certificate.

Expired key pairs are not re-issued.

1.1.5.2. High level process

The CMLC high level process is outlined in the decision tree illustrated below.

Figure 1.2 CMLC High Level Process



1.1.5.3 Generation

The CAPL PKI generates Certificates upon receipt of an authorised and validated request for:

1. new Certificates;
2. Certificate renewal.

Generation involves:

1. receipt of an approved and verified Certificate request;
2. creating a new Certificate;
3. binding the Key Pair associated with the Certificate to a Certificate owner;
4. issuing the Certificate and the associated Public Key for operational use under:
 - a Distinguished Name associated with a Certificate owner; and,
 - a recognised and relevant CP.

Generation is performed in a physically secure facility, on the receipt of a properly

authorised digital Certificate request. Certificate requests are initiated only by approved Registration Authorities (RA).

In making Certificate requests, the RA will be bound to a CA³ to:

1. confirm that the user's name does not appear in its list of compromised users;
2. comply with a nominated registration procedure in a CP including verification of identification and/or employment;
3. comply with all privacy requirements;
4. obtain approval to make a Certificate request;
5. obtain an acknowledgement that the Certificate Details can be published on a directory service.

Certificate owner names are unique and comply with the X.500 standard for Distinguished Names.

An audit process operates to ensure that CAPL PKI complies with the requirements of the Gatekeeper Accreditation process.

The RA requesting Certificate generation acts as a trusted third party in verifying:

1. the relationship between the key pair and the Certificate owner;
2. the identity and any designated attributes or characteristics of the Certificate owner.

1.1.5.4 Operational use

A Certificate comes into operational use at the time of issue, and remains in operational use until it:

1. expires; or,
2. is suspended or revoked.

A Certificate that is suspended returns to operational use if the suspension is withdrawn, or if a notice of revocation is not received by the end of a period of time, known as the "grace period".

1.1.5.5. Certificate lifetimes

Certificates have a fixed operational lifetime that is determined by the CAPL PAA. Subordinate CAs and RAs in the CAPL PKI are only enabled to support specific Certificate profiles including validity date and periods.

The validity period of a Certificate depends on its intended usage and the policy domain within which it is issued. All Certificates are issued with a designated expiry date.

³ This may take the form of a Contract where the CA and RA are in separate legal entities, or a process where the CA and RA are within the same legal entity

1.1.5.6 Expiry

Certificates expire automatically upon reaching the designated expiry date, at which time the Certificate is archived.

Note that:

1. the life of a Certificate can not be and is not extended;
2. expired Certificates can not be and are not re-issued.

1.1.5.7 Archive

Expired Certificates are archived for a minimum period of seven years from the date of expiry, unless another period is specified in the relevant CP.

1.1.5.8 Compromise

Certificates in operational use that become compromised are revoked in accordance with a defined procedure. Certificates are deemed to be compromised when the integrity of the Private Key associated with the Certificate is in doubt.

Consistent with a nominated CP Certificates remain in the compromised state for only such time as it takes to arrange for revocation.

1.1.5.9 Suspension

A Suspension notice warns PKI users that a particular Certificate is under investigation for a limited period of time, known as the “grace period”.

Suspension is used as interim step before revocation is effected and involves issuing a notice to PKI users advising:

1. that a Certificate is under investigation;
2. the period during which the suspension applies.

The Suspension notice appears on a nominated CAPL PKI X.500 Directory. The notice does not set out the reasons for suspension or the results of any investigation. Only the fact of the suspension is provided.

1.1.5.10 Revocation

Certificate revocation permanently invalidates any trusted use of a Certificate.

Certificates are revoked when:

1. there is a compromise of the Certificate owner's Private Key;
2. there is a misrepresentation or errors in the Certificate;
3. the Certificate is no longer required, including Employee Certificates that are no longer required because the employee has left the employment of the user organisation, etc.

Revoked Certificates are added to the CAPL PKI X.500 Directory Certificate Revocation List (CRL).

1.1.5.11 Operational compliance

All Certificate operations comply with:

1. the policy requirements of:
 - a CAPL recognised Certificate Policy Statement (CP);
 - a CAPL approved and recognised CPS;
 - a CAPL approved and recognised Certificate Profile;
 - published and internal privacy policies and practices;
 - published and internal security policies and practices;
2. the technology requirements of:
 - relevant internal guidelines for the physical protection of technology assets;
 - X.500 Directory services;
 - X.509 Certificate format;
 - X.509 Certificate Revocation List (CRL) format;
 - X.500 Distinguished name standards;
 - PKCS#7 format for Digital Encryption and Digital Signatures;
 - PKCS#10 Certificate Request format;
 - recognised PKI conventions and standards;
3. legal requirements of domestic and, where applicable, international privacy legislation;
4. appropriate international and domestic standards relevant to PKI operations;
5. audit requirements for PKI and/or Certificate operations.

1.1.6 PKI Operational Infrastructure

1.1.6.1. The CAPL PKI operational infrastructure:

1. uses CAPL approved products from a PKI product provider. These products automate key and Certificate management functions;
2. employs a common architectural model under which Certification and Registration functions are separated.

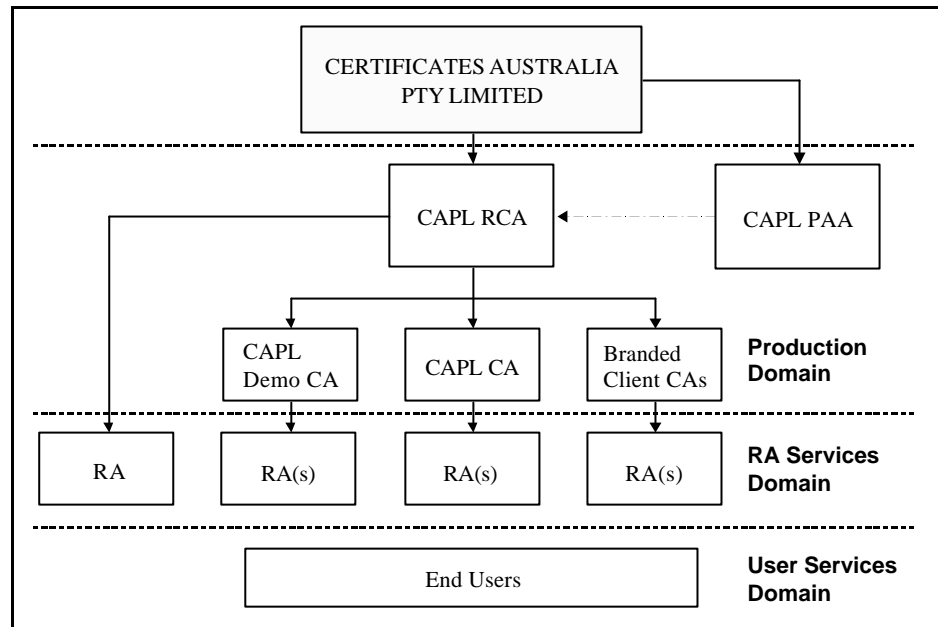
The CAPL PKI operational infrastructure comprise three distinct domains:

1. Production Domain, (including the RCA, ICA and OCA environment);

2. RA Services Domain;
3. User Services Domain.

Figure 1.3 below provides a diagrammatic representation of these domains, which is followed by explanatory text.

Figure 1.3 CAPL PKI Operational Infrastructure



1.1.6.2. Production domain

The hierarchy in the Production Domain consists of the CAPL RCA and all CAs that are operated by CAPL. The RCA establishes and maintains the PKI while the CAs are responsible for issuing Certificates.

There are two types of CA within this domain:

1. CAs managed by CAPL (“CAPL CAs”) including ICAs;
2. CAs managed by customers (“Branded Client CAs”).

1.1.6.3. RA service domain

The RA Services Domain consists of all RAs that are operated under the CAPL hierarchy. These RAs are responsible for supplying user registration and key generation services to End Entities.

1.1.6.4. User service domain

The User Services Domain includes End Entities, who use or rely on Certificates for authentication, integrity non-repudiation and confidentiality.

1.1.6.5 Validation of digital signatures

The End Entity product selected for use within and supported by the CAPL PKI provides the following functions:

1. verification that the digital signature has been created by the Private Key bound to the Certificate listed for the signing party in the CAPL X.500 Directory;
2. a mechanism by which the message, transaction or other file (“signed file”) may be checked to determine that it has not been altered since the digital signature was appended.

The End Entity product can accomplish these functions by:

1. establishing a Certificate chain⁴ for validation of the signature, commencing with the signing party’s Certificate and ending with the RCA’s Certificate. Note that it is possible to establish more than one Certificate chain for a signature, through cross-certification.
2. where more than one Certificate chain can be established, the End Entity product can be utilised to:
 - allow the End Entity various options to manually establish the chain; or,
 - establish a chain through a series of user-defined preferences; or,
 - establish the shortest possible chain; or,
 - validate all possible chains.
3. validating all Certificates in the established chain(s);
4. application of a hash function to the signed file;
5. comparing the resulting hash to the hash that is appended to the signed file, produced using the signing party’s Private Key.

The Relying Party is able to verify:

1. the validity of the transaction, by inspecting the signing party’s CP to ensure the signing party has acted:
 - in a valid and authorised manner in terms of the Certificate usage allowed by the CP;
 - in compliance with any special requirements of the CP.
2. at their own discretion whether the Certificate has been revoked, by checking the CRL in the X.500 Directory.

1.1.7 Scope

The practices described in this CPS are:

1. based upon but not limited to, the roles, responsibilities, duties and obligations contained within CAPL Gatekeeper compliant and GPKA accredited CP;

⁴ A list of Certificates, typically commencing with an End Entity Certificate, then progressing to the Certificates of the End Entity’s RA, the issuing CA, and the RCA.

2. binding upon all parties within the CAPL PKI, through the inter-linking contractual responsibilities, obligations and duties between:
 - the CAPL RCA and its subordinate CAs;
 - CAs and their subordinate RAs;
 - RAs and their registered End Entities.

This CPS incorporates information from other documents regarding practices involved in the issue, use and validation of Certificates, and in the operational maintenance of the PKI infrastructure. It includes, but is not limited to the:

1. Certificate categories that may be created;
2. functions and obligations of CAPL;
3. registration of End Entities;
4. functions and obligations of End Entities;
5. process of approving new Certificate categories and Certificate policy.

1.1.8 Security Philosophy

The security philosophy governing the operational management of the CAPL PKI is:

“Prevention, Detection and Considered Response”.

‘Considered response’ describes the execution of such actions as are justified having considered all the circumstances.

This philosophy means that the first aim of the CAPL PKI is:

1. to prevent any unauthorised action taking place;
2. should an unauthorised action take place, to be able to detect and record the unauthorised event or action;
3. finally, to respond to unauthorised events or actions in a considered and positive manner.

In all cases, CAPL PKI operates to:

1. securely generate their Private Keys and take adequate precautions to protect against their compromise, modification, disclosure, loss or unauthorised use;
2. be able to detect and record unauthorised events and actions.

1.1.9 Staffing Arrangements

The CAPL PKI has adopted and employs personnel and management practices to ensure the trustworthiness, integrity and professional conduct of its staff. CAPL complies with Gatekeeper requirements for the vetting of its operations staff by the Australian Security Vetting Service (ASVS).

The following personnel standards are applied:

1. the minimum standard for personnel vetting is:

HIGHLY PROTECTED

2. all CAPL operations staff enter into non-disclosure agreements to protect against the unauthorised disclosure of confidential information;
3. all CAPL operations staff are trained in:
 - basic PKI concepts;
 - the use and operation of CA or RA software;
 - documented CA and RA procedures;
 - computer security awareness and procedures;
 - for pertinent CA staff, how to explain to RA Certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
 - for pertinent RA staff, how to explain to End Entity Certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
 - the meaning and effect of the legal contract their Service Provider has signed with its superior entity;
 - the meaning and effect of relevant CP, this CPS and for pertinent RA staff, the Subscriber agreement.

1.1.10 Right of Inquiry

CAPL reserves the right to make reasonable inquiry in accordance with arrangements agreed with the customer to determine the validity of a suspension or revocation request.

1.2 Identification

This CPS is referred to as the “Certificates Australia CPS”.

Object Identifiers (OID) are not applicable to CPS documents.

1.3 Community and Applicability

CAPL has established a Root Certification Authority (RCA) under which a number of subordinate CAs and RAs operate.

These subordinate CA or RA services within the CAPL PKI are either:

1. managed and operated by CAPL; or,
2. managed by customers but operated by CAPL (outsourced services); or,
3. managed and operated by customers (external services).

This CPS supports:

1. all CA and RA services that operate under the CAPL RCA, i.e. that are within the CAPL “chain of trust”;
2. all types of Certificates issued under the CAPL RCA hierarchy.

As a consequence, the practices described in this document allow for a wide range and variety of:

1. Certificate types, supporting individual transactions that have differing levels of information sensitivity and financial value;
2. End Entities, who include:
 - individuals;
 - commercial or non-profit organisations;
 - state or Commonwealth Government departments, agencies or authorities;
3. CA and RA service operators.

The practices in this CPS must:

1. accommodate the diversity of the community and the scope of applicability within the CAPL chain of trust;
2. adhere to the primary purpose of the CPS, of ensuring the uniformity and efficiency of practices throughout the PKI.

In keeping with their primary purpose, the practices in this document:

1. are the minimum requirements necessary to ensure that Subscribers and relying parties have the highest possible level of assurance, and that critical functions are provided at appropriate levels of trust;
2. apply to all stakeholders, for the generation, issue, use and management of all Certificates and key pairs.

1.3.0 Policy Authorities

1.3.0.1 Government Public Key Authority (GPKA)

The GPKA oversees the operation of accredited CAs and RAs within the Gatekeeper schema.

1.3.0.2 GPKA functions

The GPKA establishes and maintains the criteria for Gatekeeper accreditation.

1.3.0.3 GPKA Contact Details

The contact details for the GPKA are published in relevant CP, including recognised CAPL CP.

1.3.0.4 Certificates Australia Pty Limited Policy Approval Authority (CAPL PAA)

The CAPL PAA has been established to maintain the integrity of the policy infrastructure in the CAPL PKI.

1.3.0.5 CAPL PAA functions

The CAPL PAA performs the following functions:

1. CP approval within the CAPL PKI;
2. ensure the integrity of PKI policy structures;
3. administer subordinate policy infrastructure to maintain the total integrity of the PKI.

1.3.0.6 CAPL PAA Contact Details

The contact details for the CAPL PAA are published in each CP within the CAPL hierarchy.

1.3.0.7 Policy Creation Authorities (PCA)

A PCA is responsible for formulating policy relating to a specific part of the CAPL PKI, for example for Certificates issued by a specific CA.

Within the CAPL PKI, the PCA function for the CAPL RCA, and the CAPL OCA is carried out directly by the CAPL PAA. A register of PCAs will be maintained by CAPL and published on its web site.

1.3.0.8 PCA functions

The PCA performs the following functions:

1. formulate new policy and policy changes within the CAPL PKI;
2. submit new or changed policies to the CAPL PAA for approval.

1.3.0.9 PCA Contact Details

The contact details for the CAPL PAA are published in each CP within the CAPL hierarchy.

1.3.1 Certification authorities

1.3.1.1 CAPL Root Certification Authority

The CAPL RCA is the highest point of trust within the CAPL PKI hierarchy. The primary purpose of the RCA is to certify subordinate Certification Authorities (CA), by digitally signing their Certificates. The CAPL RCA self-signs its own Certificate.

The RCA is accessed via a single Registration Authority (RA) which is used solely for the purpose of creating subordinate CA Certificates.

The key length of the CAPL RCA's Signing Key, used to sign Certificates, is as determined by a relevant Certificate profile. Generation of the RCA's keys is performed on a platform in a physically secure facility that meets the Gatekeeper physical security standards.

1.3.1.2 CAPL RCA Functions

The functions performed by the CAPL RCA include:

1. constitution of a PAA for the purpose of reviewing and approving policies applicable to and recognisable by, the RCA;
2. generation of its own keys;
3. issuing a self signed Certificate;
4. publication of its Public Key Certificate in the CAPL X.500 Directory services;
5. providing relying parties with access to:
 - Certificate information published in the directory services;
 - the Public Keys associated with operational Certificates that are listed in the directory services;
6. publication of its Root CA Hash on the web sites at:

www.certificates-australia.com.au

www.secdom.com.au

7. operation of the RCA in an efficient and trustworthy manner and in accordance with:
 - the CAPL CONOPS;
 - a relevant CAPL Gatekeeper compliant and GPKA accredited CP;
 - this CPS;
 - CAPL security policies;
 - documented internal operational procedures;
8. approve the naming conventions for the creation of distinguished names for Certificate applicants, in compliance with the X.500 standard for Distinguished Names;
9. administration of the registration of subordinate CAs;

10. issuance of Certificates for subordinate CAs on the receipt of authenticated digitally signed certification requests;
11. publication of issued Certificates in the CAPL X.500 Directory services;
12. to make reasonable inquiry in accordance with arrangements agreed with the customer to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level it deems warranted in its chain of trust;
13. revocation of Certificates on receipt of authenticated digitally signed revocation requests, or when its inquiries (in accordance with arrangements agreed with the customer) into the compromise or suspected compromise of a Private Key have established the validity of a revocation request;
14. posting revoked Certificates in the directory services CRL;
15. conduct of regular internal security audits;
16. conduct of compliance audits of immediately subordinate CAs when Certificate renewal is due.

1.3.1.3 CAPL RCA Contact Details

The contact details for the CAPL RCA are described and published in each CP within the CAPL hierarchy.

1.3.1.4 Certification Authorities

The primary purpose of the various CAs operating under the CAPL hierarchy is to provide Certificate management services (generation, operational use, compromise, suspension, revocation and expiry) for End Entities within their respective policy domain(s). These CAs consist of:

1. the CAPL CA, that provides Certificate management services for customers who do not wish to operate their own Certification Authority;
2. branded client CAs, that operate under a customer's name but are maintained and supported by CAPL;
3. CAs that are operated by customers on their own sites.

The key length of a CA's:

1. CA Key, used to sign Certificates is as determined by a relevant Certificate Profile;
2. Protocol Key, used to sign responses to RA requests is as determined by a relevant Certificate profile.

Generation of a CA's keys is performed on a platform in a physically secure facility that meets the Gatekeeper physical security standards.

1.3.1.5 CA Functions

CAs operating under the CAPL hierarchy perform the following functions:

1. generate their own keys;

2. submit their Public Keys together with digitally signed certification requests to the CAPL RCA;
3. publish each CP under which they issue Certificates, and this CPS on a nominated web site specified within a relevant CP. The CAPL OCA publishes relevant CP and this CPS on:

www.certificates-australia.com.au

www.secdom.com.au

4. operate the CA in an efficient and trustworthy manner and in accordance with:
 - the CAPL Concept of Operations (CONOPS);
 - an appropriate contract agreement (Note that no such agreement exists between the CAPL RCA and the CAPL CA, which are the same legal entity);
 - all CP that they issue Certificates under;
 - this CPS;
 - CAPL System Security Plan;
 - documented internal operational procedures;
5. on the receipt of authenticated digitally signed Certificate requests from CAPL authorised Registration Authorities, issue Certificates in accordance with the associated CP for:
 - RAs;
 - End Entities;
6. publish issued Certificates in a nominated X.500 Directory. The CAPL CA publishes these Certificates in the CAPL X.500 Directory;
7. make reasonable inquiry in accordance with arrangements agreed with the customer to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level they deem warranted in their chain of trust;
8. revoke Certificates on receipt of authenticated digitally signed revocation requests, or when their inquiries (in accordance with arrangements agreed with the customer) into the compromise or suspected compromise of a Private Key have established the validity of a revocation request;
9. post revoked Certificates in the directory services CRL;
10. conduct regular internal security audits;
11. conduct compliance audits of subordinate RAs when Certificate renewal is due;

12. assist in audits conducted by the RCA to validate the renewal of their own Certificates.

1.3.1.6 CA Contact Details

The contact details for CAs that operate under the CAPL hierarchy are published in each CP that they issue Certificates under, or the CP may advise a web site address or other location where the contact details may be found.

1.3.2 Registration Authorities

The primary purpose of an RA is to register End Entities. RAs have the responsibility of accepting Certificate applications, authenticating the identity or other credentials of the applicant, then approving or rejecting the application. These obligations are enforced in contract and are set out in a set of RA Operating Procedures.

Each RA within the CAPL hierarchy is subordinate to a nominated CA, this is a function of the operating hierarchy.

The key length of an RA's:

1. Authentication key, used to sign requests to a nominated CA is as determined by a relevant Certificate profile.
2. Confidentiality key, used for receiving encrypted messages, is as determined by a relevant Certificate profile.

The generation of an RA's keys is performed on a platform in a physically secure facility that meets the Gatekeeper physical security standards.

1.3.2.1 RA Functions

RAs perform the following functions:

1. generate their own keys;
2. submit their Public Keys together with digitally signed certification requests to their superior CA;
3. operate the RA in an efficient and trustworthy manner and in accordance with:
 - the CAPL CONOPS;
 - a contractual agreement (unless they are within the same legal entity, for example, the CAPL OCA and CAPL RA);
 - each CP that it accepts Certificate applications under;
 - this CPS;
 - its internal security and privacy policies;
 - documented operational procedures;
4. register Subscribers including:

- authenticating material Certificate information, For example: such as sighting Evidence of Identity (EOI) documentation;
 - proposing and approving distinguished names for Certificate applicants;
 - confirming that a Certificate applicant's name does not appear in their list of compromised users;
 - generating key pairs for Certificate applicants, or accepting Subscriber generated keys provided the Subscriber can both prove possession of and establish their right to use the key pairs;
 - ensure that a Subscriber signs an Subscriber Agreement and, where appropriate, a relying party agreement;
5. submit Subscriber Public Keys together with digitally signed certification requests to their superior CA, and receive the Certificates issued in accordance with these requests;
 6. issue keys and Certificates to Subscribers, ensuring that Private Keys and PICs are not obtained by third parties prior to being received by the Subscriber, and that Private Keys are not captured by any other mechanism under the control of the RA;
 7. authenticate requests from Subscribers for the renewal or revocation of their Certificates, and generate digitally signed renewal or revocation requests to their superior CA;
 8. may notify Subscribers of the imminent expiry of their Certificates. Where such a service is provided, Subscribers are not to rely upon the RA's notification but are to retain sole responsibility for requesting Certificate renewal before the expiry of their current Certificates;
 9. make reasonable inquiry in accordance with arrangements agreed with the customer to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level they deem warranted in their chain of trust;
 10. process certificate revocations on receipt of authenticated digitally signed revocation requests, or when their inquiries (in accordance with arrangements agreed with the customer) into the compromise or suspected compromise of a Private Key have established the validity of a revocation request;
 11. maintain a list of suspended or revoked Keys and Certificates, and periodically provide these to an X.500 directory to ensure their publication in a CRL;
 12. conduct regular internal security audits;
 13. assist in audits conducted by their superior CA to validate the renewal of their own Certificates.

1.3.2.2 RA Contact Details

The contact details for RAs that operate under the CAPL hierarchy are published in each relevant CP that they issue Certificates under, or the CP may publish a web site address or other location where the contact details may be found.

1.3.3 End Entities

End Entities may be Commonwealth Government agencies that act in the name of the Commonwealth of Australia (e.g. Office for Government Online), statutory authorities (which are entities that are legally separate from the Commonwealth of Australia) or corporate or natural persons.

An End Entity acts as a Subscriber when they use their keys to encrypt and/or digitally sign a message, transaction or other electronic file.

An End Entity acts as a relying party when they rely on another user's Public Keys to decrypt and/or authenticate a message, transaction or other electronic file.

The key length of an End Entity's Authentication and Confidentiality keys are required to be fully compliant with the Gatekeeper schema.

Where End Entity key pairs are generated by:

1. RAs, generation is to be performed on a platform in a physically secure facility;
2. End Entities, reasonable security measures are to be taken to ensure the protection of their Private Keys against compromise.

1.3.3.1 End Entity Functions

End Entity (i.e. End Entity) functions are defined in the relevant Subscriber Agreement and, in the case of third party relying parties, the relevant Third Party Relying party agreement.

1.3.3.2 End Entity Contact Details

The following End Entity contact details may be published in an End Entity's Public Key Certificate in compliance with X.509 standards:

1. organisation name and department name in the End Entity's Distinguished Name in the Subject field;
2. the End Entity's e-mail address, or Universal Resource Location (URL) may be published in the Subject Alternative Name field.

End Entity contact information is maintained by the End Entity's RA.

1.3.4 Applicability

Certificates issued by the CAPL RCA are used to support secure electronic commerce and the secure exchange of information by electronic means:

1. between Government Agencies, business, charitable bodies, professional organisations, strata schemes, sporting associations, community bodies, special interest groups, registered clubs and private individuals in any combination;

2. within both closed and open PKI communities.

The practices described in this CPS support a large, diverse and widespread community of users who require PKI Certificate services in support of electronic transactions and information services.

The CAPL PKI user community may regard the practices described in this CPS as:

1. ensuring standard operating procedures and uniform quality of service delivery across the PKI;
2. fostering and promoting high levels of trust and integrity across the PKI.

1.3.4.1 Gatekeeper restrictions

Under the Gatekeeper schema, the use of each type and grade of Certificate is generally restricted to a specified level of:

1. sensitivity of information; and,
2. financial value.

These restrictions are detailed in the table below.

Certificate		Applicable use	
Type	Grade	Sensitivity of information	Financial value
1	1	Non-sensitive information.	No financial implications.
	2	IN CONFIDENCE.	Individual transactions up to \$1,000.
	3	PROTECTED/ RESTRICTED.	Individual transactions up to \$10,000.
2	1	Non-sensitive information.	Individual transactions up to \$10,000.
	2	IN CONFIDENCE.	Individual transactions greater than \$10,000 with a maximum aggregate of \$100,000.
	3	PROTECTED/ RESTRICTED.	Individual transactions greater than \$10,000 with a maximum aggregate of \$100,000.

These general conditions may be varied in a particular implementation to take account of:

- The intended use of the certificate;
- The intended community of interest;
- Review by the GPKA

1.3.4.2 Applicable Certificate usage

The CAPL RCA supports a variety of functional classes. Typically Certificates supported by this CPS fall into one or more of the primary functional classes set out below:

1. “Identity“ Certificates;
2. “Financial“ Certificates;
3. “Attribute“ Certificates;
4. “Functional“ Certificates.

Within each of these classes, different assurance levels apply, or different attributes are used.

Gatekeeper compliant and GPKA accredited Certificates may encompass all of the abovementioned Certificate classes. Within nominated policy domains, Certificates may also be used for multiple purposes.

Table of functional Certificate classes

Class	Purpose	Assurance levels
Identity	Authenticates Certificate holder's identity through a rigorous EOI process.	Low, medium and high.
Financial	Authorises Certificate holder to initiate financial transactions of a certain type and limit.	Low, medium and high.
Attribute	Associates Certificate holder with pre-defined access rights and system privileges.	Not applicable as levels of access, etc. are defined within Certificate attributes.
Functional	Identifies Certificate holder's function or role.	Low, medium and high.

1.3.4.3 Identity Certificates

Identity Certificates authenticate the identity of the person or organisation to whom they are issued. Designated uses include:

1. within messaging systems, to authenticate the identity of a person or organisation sending a message and to provide assurance that subsequent communications are from the same person or organisation;
2. in secure electronic data exchange, to authenticate and protect sensitive information.

The criteria used by an RA for the authentication of a Certificate owner's identity depend upon:

1. the type of Certificate, i.e. individual, organisation or employee;
2. the grade of Certificate, i.e. Grade 1, 2 or 3;
3. The reliance level (if any) of the Certificate.

1.3.4.4 Financial Certificates

Financial Certificates are issued to authorise and verify a range of financial transactions to a given monetary limit and for designated purposes.

1.3.4.5 Attribute Certificates

Attribute Certificates bind the Certificate owner to one or more attributes associated with the Certificate owner. Designated uses include:

1. the Certificate owner's relationship with an organisation;
2. logon rights or directory privileges associated with the Certificate Owner;
3. the role of an individual or other entity.

1.3.4.6 Functional Certificates

Functional Certificates are issued to entities including but not limited to individuals and organisations, to facilitate the performance of a specific function or group of functions. Designated uses include functional Certificates issued to facilitate:

1. the automatic processing of transactions by a file server;
2. the provision of certification services by CAPL PKI service providers;
3. the identification of an Entity that does not fall within the definition of Identity Certificate Class.

1.3.4.7 Restricted Certificate usage

Specific restrictions on the use of a Certificate are contained in the CP under which the Certificate is issued. These restrictions may, for example, limit or prescribe the:

1. community of interest;
2. conditions which must be satisfied before a Certificate is used;
3. actual usage of the Certificate;
4. processing steps or other actions which are to be performed after a Certificate has been used.

Parties within the CAPL PKI are to use Certificates only in the manner, and for the purposes prescribed in a relevant CP. Any use of a Certificate in a manner or for a purpose not in accordance with a relevant CP is not recognised nor supported by this CPS.

1.4 Contact Details

1.4.1 Specification administration organisation

This CPS is administered by Certificates Australia Pty Limited.

1.4.2 Contact person

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

**General Manager - Certificates On-Line
Certificates Australia Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
2060 AUSTRALIA**

E-mail may be sent to:

info@certificates-australia.com.au

1.4.3 Person determining CPS suitability for this policy

See 1.4.2 *Contact person*.

2. GENERAL PROVISIONS

CAPL operates Gatekeeper PKI accordance with the Gatekeeper accredited documents.

2.1 Obligations

Certificate owners are:

1. advised through the CP of their duties and obligations to ensure the safety, protection and integrity of their Private Keys;
2. required for specific classes of Certificates to enter into an agreement that clearly defines these obligations;
3. not to interfere with or damage, or attempt to interfere with or damage, the operational infrastructure of the CAPL PKI or any component thereof. The CAPL PKI has:
 - been structured and is operated in such a manner as to minimise the risk of compromise or wilful damage by a Certificate owner;
 - defined a security policy that provides for the early detection of an attempt to damage the infrastructure and to collect sufficient evidence for a prosecution.

2.1.0 CAPL Obligations

Changes to this CPS can only be made at the direction of the General Manager – Certificates On-Line. Factors that will normally result in change requests include, but are not limited to:

1. a mandated change to a GPKA Accreditation requirement; or,
2. a change in the technology supporting the PKI (e.g. ITSEC E3 EPL Approval); or,
3. a change required to ensure compliance with published international and Australian standards.

2.1.0.1 CAPL PAA Obligations

The CAPL PAA has no Certificate practice obligations under this CPS. The CAPL PAA's general obligations in regard to approving CP and maintaining the CAPL PKI policy infrastructure are detailed in a relevant CP.

2.1.0.2 RCA Obligations

The CAPL RCA discharges its obligations under this CPS by:

1. providing CA, RA and other software applications through Baltimore Pty Limited;

2. providing the CAPL PKI operational infrastructure and certification services, including X.500 Directory and service provider software (through Baltimore Pty Limited);
3. making reasonable efforts to ensure it conducts an efficient and trustworthy operation. “Reasonable efforts” includes but does not limit the RCA to operating in compliance with:
 - documented internal operational procedures;
 - this CPS;
 - within applicable law;
4. approving the establishment of all new CAs at any level in the CAPL hierarchy and on approval, executing an RCA-CA operating agreement;
5. maintaining this CPS and enforcing the practices described within it;
6. publishing its Root CA Hash on the Certificates Australia web site and other nominated web sites;
7. issuing Certificates to authorised CAs, that comply with X.509 standards and are suitable for the purpose required;
8. issuing Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
9. publishing issued Certificates without alteration in the X.500 Directory;
10. making reasonable inquiry in accordance with arrangements agreed with the customer to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level it deems warranted in its chain of trust;
11. revoking Certificates on receipt of authenticated digitally signed revocation requests, or when its inquiries (in accordance with arrangements agreed with the customer) into the compromise or suspected compromise of a Private Key have established the validity of a revocation request;
12. promptly notifying Certificate owners in the event it initiates revocation of their Certificates;
13. conducting compliance audits of immediately subordinate CAs when Certificate renewal is due.

2.1.0.3 ICA Obligations

ICAs operating under the CAPL hierarchy discharges their obligations under this CPS by:

1. making reasonable efforts to ensure it conducts an efficient and trustworthy operation. “Reasonable efforts” includes but does not limit the RCA to operating in compliance with:
 - documented internal operational procedures;

- this CPS;
 - within applicable law;
2. approving the establishment of all new CAs at any level in the CAPL hierarchy and on approval, executing an RCA-CA operating agreement;
 3. maintaining this CPS and enforcing the practices described within it;
 4. publishing its Root CA Hash on the Certificates Australia web site and other nominated web sites;
 5. issuing Certificates to authorised CAs, that comply with X.509 standards and are suitable for the purpose required;
 6. issuing Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
 7. publishing issued Certificates without alteration in the X.500 Directory;
 8. making reasonable inquiry in accordance with arrangements agreed with the customer to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level it deems warranted in its chain of trust;
 9. revoking Certificates on receipt of authenticated digitally signed revocation requests, or when its inquiries (in accordance with arrangements agreed with the customer) into the compromise or suspected compromise of a Private Key have established the validity of a revocation request;
 10. promptly notifying Certificate owners in the event it initiates revocation of their Certificates;
 11. conducting compliance audits of immediately subordinate CAs when Certificate renewal is due.

2.1.1 CA Obligations

CAs operating under the CAPL hierarchy discharge their obligations under this CPS by:

1. making reasonable efforts to ensure they conduct an efficient and trustworthy operation. “Reasonable efforts” includes but does not limit the CA to operating in compliance with:
 - a contractual agreement;
 - documented internal operational procedures;
 - applicable CP;
 - this CPS;
 - within applicable law;
2. approving the establishment of subordinate RAs and on approval, (where appropriate) an operating agreement or procedure;

3. enforcing within the sphere of their operations the practices described within this CPS, or an approved CPS relevant to the CA operating environment;
4. publishing applicable CP and this CPS on the web site(s) nominated in the CP;
5. upon receipt of a valid Certificate request, issuing Certificates which comply with X.509 standards and meet the requirements of the request;
6. issuing Certificates that are factually correct from the information known to them at the time of issue, and that are free from data entry errors;
7. publishing issued Certificates without alteration in a nominated X.500 Directory;
8. making reasonable inquiry in accordance with arrangements agreed with the customer to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level they deem warranted in their chain of trust;
9. revoking Certificates on receipt of authenticated digitally signed revocation requests, or when their inquiries (in accordance with arrangements agreed with the customer) into the compromise or suspected compromise of a Private Key have established the validity of a revocation request;
10. promptly notifying Certificate owners in the event the CA initiates revocation of a Certificate;
11. maintain a list of suspended or revoked Keys and Certificates, and periodically provide these to an X.500 directory to ensure their publication in a CRL.
12. conducting compliance audits of immediately subordinate CAs and RAs when Certificate renewal is due in accordance with published standards agreed by CAPL and the GPKA;
13. assisting in audits conducted by the RCA to validate the renewal of their own Certificates.

2.1.2 RA Obligations

RAs operating under the CAPL hierarchy discharge their obligations under this CPS by:

1. making reasonable efforts to ensure they conduct an efficient and trustworthy operation. “Reasonable efforts” includes but does not limit the RA to operating in compliance with:
 - a contractual agreement;
 - documented internal operational procedures;
 - applicable CP;
 - this CPS;
 - within applicable law;
2. enforcing within the sphere of their operations the practices described within

this CPS;

3. accepting End Entity Certificate applications, including authenticating material (including where relevant EOI), Certificate information, obtaining a Subscriber agreement and, where required, a relying party agreement, and accepting or rejecting the application;
4. where required, archiving private confidentiality keys they have generated;
5. verifying the integrity and possession of, and establishing the End Entity's right to use, user generated keys presented for certification;
6. advising End Entities of their obligations under the relevant CP, this CPS and the appropriate Subscriber agreement and relying party agreement, and providing End Entities with copies of the relevant CP and this CPS or advising them how these documents may be accessed;
7. submitting Certificate requests that comply with X.509 standards and meet the requirements of approved Certificate applications;
8. submitting Certificate requests that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
9. issuing keys and Certificates to End Entities and ensuring that the Private Keys and key transport access control mechanisms are not obtained by third parties prior to being received by the End Entity, and that Private Keys are not captured by any other mechanism under the control of the RA;
10. inquiring (in accordance with arrangements agreed with the customer) into any suspected compromise which may threaten the integrity of the PKI at any subordinate level within its chain of trust;
11. revoking Certificates in terms of section 4.4.1 - *Circumstances for revocation*;
12. promptly notifying Certificate owners in the event it initiates revocation of their Certificates;
13. maintaining a list of compromised keys and compromised users. The compromised list is to include relevant information regarding the identity of the individual(s) concerned, reasons and causes for inclusion on the list and such other information as might be required to minimise damage or liability to all CAPL End Entities. This information is to be protected in accordance with the Commonwealth's Information Privacy Principles;
14. keeping such registration records as may be required;
15. assisting in audits conducted by the CAPL CA to validate the renewal of its own Certificates;
16. In addition, authorised CAPL RAs are required to operate within the relevant Gatekeeper standards.

2.1.3 Subscriber Obligations

Subscribers discharge their obligations under this CPS by:

1. providing their RA with true and correct information at all times;
2. providing sufficient proof of material Certificate information to meet user registration or Certificate renewal requirements;
3. requesting generation of End Entity keys or requesting acceptance of self generated keys;
4. proving possession of and establishing their right to use, self-generated keys;
5. acknowledging that in making a Certificate application, they are consenting to Certificate issue in the event the application is approved;
6. agreeing to their Public Keys and Certificates being published in the CAPL directory services as part of Certificate issue;
7. signing a Subscriber agreement where required by a relevant CP;
8. immediately notifying their RA of any error or defect in their Certificates, or of any subsequent changes in the Certificate information;
9. reading the applicable CP and this CPS before using their key pairs;
10. using their keys pairs and other End Entity's Public Keys only in accordance with a relevant CP;
11. ensuring the safety and integrity of their Private Keys, including:
 - controlling access to the computer containing their Private Keys;
 - protecting the access control mechanism used to access their Private Keys;
12. immediately notifying their RA of any instance in which a key pair is compromised or in which they have reason to believe a key pair may have become compromised;
13. exercising due diligence and reasonable judgement before deciding to rely on a digital signature, including whether to check on the status of the relevant Certificate;
14. regularly enquiring on the status of Certificates, by checking the CRL.

2.1.4 Relying party obligations

Relying Party obligations are set out in the End Entity Subscriber Agreement. A Relying Party shall have the following obligations:

- they understand the extent to which the Certificate can be relied upon;
- they are aware of the CP supporting the Certificate relied upon;
- they are aware of the limitations (if any) of the Certificate upon.
 - exercise due diligence and reasonable judgement before deciding to rely on a digital signature. As a minimum, the End Entity should satisfy themselves that:

- the Certificate is still valid, e.g. CRL check
- the Certificate is appropriate for the transaction type;
- the integrity of the message has not been compromised (application dependant).

2.1.5 Repository Obligations

The CAPL Repository functions are performed by the X.500 Directory.

The CAPL RCA provides and maintains the operational infrastructure for the X.500 Directory, and CAs operating under the CAPL RCA post Certificates and CRLs to the Directory.

Repository obligations are therefore incorporated into sections 2.1.0.2 *RCA Obligations* and 2.1.1 *CA Obligations*.

2.2 Liability

CAPL has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

1. inhibit misuse of those resources by authorised personnel;
2. prohibit access to those resources by unauthorised individuals.

These measures include but are not limited to:

1. identifying contingency events and appropriate recovery actions in a Contingency & Disaster Recovery Plan;
2. performing regular system data backups;
3. performing a backup of the current operating software and certain software configuration files;
4. storing all backups in secure local and offsite storage;
5. maintaining secure offsite storage of other material needed for disaster recovery;
6. periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
7. periodically reviewing its Contingency & Disaster Recovery Plan, including the identification, analysis, evaluation and prioritisation of risks;
8. periodically testing uninterrupted power supplies.

2.2.0 CAPL Liability

Please refer the relevant CP.

2.2.0.1 CAPL PAA Liability

Please refer the relevant CP.

2.2.0.2 CAPL RCA Liability

Please refer the relevant CP.

2.2.1 CA Liability

Please refer the relevant CP.

2.2.2 RA Liability

Please refer the relevant CP.

2.2.3 End Entity Liability

Please refer the relevant CP.

2.3 Financial responsibility

Please refer the relevant CP.

2.3.1 Indemnification by relying parties

Please refer the relevant CP.

2.3.2 Fiduciary relationships

Please refer the relevant CP.

2.3.3 Administrative processes

Please refer the relevant CP.

2.3.4 Certificates Australia Pty Limited

Certificates Australia Pty Limited is a wholly owned subsidiary of Baltimore Pty Limited, a company incorporated in Australia. Baltimore Pty Limited is a wholly owned subsidiary of Baltimore Inc, a company publicly listed company on the London stock exchange.

2.3.5 Client managed CA and RA services

CAPL customers who manage CA and/or RA services under the CAPL CA must be able to meet Gatekeeper accreditation standards.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

This CPS will be governed by the law specified within the relevant CP.

2.4.1.1 Applicable contract structure

The contractual structure that underpins the policies and practices described in this document include the:

Head Agreement: Establishes a contractual relationship between CAPL and the Commonwealth of Australia represented by the Office for Government Online for the provision of CA Services.

Services Agreement: Describes contractual arrangements under which CAPL will offer Gatekeeper Services and includes the roles and responsibilities of each party. As part of this document, CAPL shall provide a copy of the Concept of Operations document.

Product Licensing Agreement: Describes the licence terms and conditions of products sold to CAPL customers and which are operated in conjunction with a CAPL CA Service Provider's services.

Customer (Agency) Agreement: Describes the contractual arrangements under the Endorsed Supplier Head Agreement and the Office for Government Online Head Agreement Framework that are put in place between the Customer and CAPL for the acquisition Certification Services. This would include specific arrangements such as: services, service levels, etc.

End Entity Subscriber Agreement: Establishes a contractual relationship between RA's and End Entities for the provision of services by the RA and between an End Entity and other End Entities, such as relying parties, who rely upon the proffered End Entity Certificate.

2.4.2 Severability, survival, merger, notice

2.4.2.1 Severability

Please refer the relevant CP.

2.4.2.2 Survival (Continuing obligations and assignment)

Please refer the relevant CP.

2.4.2.3 Merger

Please refer the relevant CP.

2.4.2.4 Notice

Please refer the relevant CP.

2.4.2.5 Notice action

Please refer the relevant CP.

2.4.2.6 Notice acknowledgement

Please refer the relevant CP.

2.4.3 Dispute resolution procedures

2.4.3.1 Hierarchy of Certificate policy

Each CP includes a statement on the hierarchy of Certificate policy.

2.4.3.2 Process

Each CP includes a statement on policy.

2.5 Fees

Please refer the relevant CP.

2.5.1 Certificate issuance or renewal fees

Please refer the relevant CP.

2.5.2 Certificate access fees

Please refer the relevant CP.

2.5.3 Revocation or status information access fees

Please refer the relevant CP.

2.5.4 Fees for other services such as policy information

Please refer the relevant CP.

2.5.5 Refund policy

Please refer the relevant CP.

2.6 Publication and repository

2.6.1 Publication of CA information

This CPS is published under the International Standard Book Number (ISBN) system.

2.6.1.1 Electronic Publication

This CPS is published electronically in PDF format on the Certificates Australia and other nominated web sites at:

www.certificates-australia.com.au

www.secdom.com.au

The PDF file is downloadable from the web site.

2.6.1.2 Hard Copy Publication

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

**General Manager - Certificates On-Line
Certificates Australia Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
2060 AUSTRALIA**

2.6.1.3 Publication by CAs

All relevant CAs within the CAPL PKI must:

1. publish this document on the web site(s) where they publish their CP; or,
2. provide a link on their CP web site(s) to the Certificates Australia web site, with an appropriate explanation that the link may be used to access a copy of this document.

2.6.2 Frequency of publication

Publication frequency is as follows:

1. Newly approved versions of CP and this CPS are published promptly;
2. Certificates are published promptly following their generation and issue;
3. CRL Publication is in accordance with section 4.4.9 *CRL Issuance Frequency*.

2.6.3 Access controls

There are no access controls on the reading of this CPS or of relevant CP on the web sites nominated for publication.

Access to Certificate information (including CRLs) within the X.500 Directory is limited to a single name search enquiry.

Appropriate access controls are used to restrict to authorised personnel the ability to write to or modify these items.

2.6.4 Repositories

The Repository for the CAPL PKI is provided through the CAPL X.500 Directory or another endorsed Directory or repository. This directory contains Certificate information for all Certificates issued within the CAPL PKI.

The Directory does not contain any information of a confidential nature.

The CAPL X.500 Directory is a high availability service that provides relying parties with Certificate information services. The directory provides the following repository services to authorised enquirers:

1. advice of Certificate status, including:
 - access to the CAPL CRL for revoked Certificates;
 - access to notices of suspension for suspended Certificates;
2. download facility for all service provider and End Entity Certificates.

The directory services provided to an enquirer may span:

1. a single policy domain; or,
2. nominated policy domains; or,
3. all policy and Certificate domains.

A directory may also include On-Line Certificate Status Protocol (OCSP) functionality.

2.6.4.1 X.500 Directory Functions

The X.500 Directory performs the following functions:

1. allow a name search enquiry on master directories or copies thereof to determine within the span of the directory structure:
 - if agreed with the Subscriber, the number of Certificates held by the nominated person;
 - the type or grade of each Certificate;
 - the status of each Certificate, i.e. valid, revoked or expired.
2. provide access to Public Keys via Certificate download;
3. automatically check the CRL prior to a Certificate being downloaded and advise the requesting party if the Certificate has been revoked.

The CAPL X.500 Directory shall not publish information about:

1. how or why a Certificate has been revoked
2. any information pertaining to an End Entity not contained in the Certificate, unless the End Entity agrees to publish such information;

3. CAPL, by agreement with its customers, may post Certificate information, and CRL to another designated Repository or Directory.

2.6.4.2 X.500 Directory Contact Details

The contact details for the X.500 Directory are published in each CP within the CAPL hierarchy.

2.6.4.3 X.500 Directory Availability

Standard availability for the X.500 Directory is during standard business hours, i.e. 9:00 a.m. – 5:00 p.m. Monday to Friday, Australian Eastern Standard Time (AEST) or Australian Eastern Daylight Savings Time (AEDST) as applicable.

A Premium service is available under a customer agreement that provides 7 days x 24 hours availability.

2.6.4.4 Restrictions on X.500 Directory access and services

Access to Certificate information is limited to a single name search enquiry that accesses the master directory or a copy thereof. The search enquiry allows an enquirer to determine within the span of the directory services provided:

1. if agreed by the Subscriber, the number of Certificates held by the nominated person;
2. the type or grade of each Certificate;
3. the status of each Certificate, i.e. valid, revoked or expired.

The repository does not:

1. provide access to End Entities in any manner other than that stated in this CPS;
2. provide any information or services to End Entities other than that information and those services listed in this CPS;
3. alter any Certificate details or notices that it receives.

Where OCSP responder functions are available with a Directory service, public access to the Directory may be denied, and access only to the OCSP Responder provided for certificate status checking purposes.

2.6.4.5 Repository publication

The CAPL Repository promptly publishes new Certificates and changes in Certificate status, including revocation, notices of suspension and expiry.

The X.500 Directory is published on the Certificates Australia and other nominated web sites at:

www.certificates-australia.com.au

www.secdom.com.au

Copies of the Directory may be published at such other locations as are required for the efficient operation of the CAPL PKI and as may be prescribed in various CP. These copies may contain the whole of the Directory structure or parts thereof.

Where OCSP responder functions are available with a Directory service, public access to the Directory may be denied, and access only to the OCSP Responder provided for certificate status checking purposes.

2.6.4.6 CRL publication

Customer operated CAs may independently publish full CRLs applicable to their policy domain(s) and/or regular notifications of newly revoked Certificates, e.g. daily or weekly lists.

CRLs published in this manner:

1. may be in any form expedient to the purposes of the CA, for example in an X.500 Directory, on paper or as e-mail messages;
2. do not form part of the CAPL Repository. CAPL is not liable for the publication of CRLs published by customer operated CAs or any consequence of malfeasance, tort or contractual breach arising from the publication thereof.
3. will not preclude End Entities from using the CAPL X.500 Directory.

Where OCSP responder functions are available with a Directory service, public access to the Directory may be denied, and access only to the OCSP Responder provided for certificate status checking purposes.

2.7 Compliance Audit

2.7.0 GPKA Evaluation

CAPL has been Accredited by the Government Public Key Authority in accordance with the GPKA's criteria and following evaluation by a team of independent evaluators.

The evaluation criteria have been defined by the Government Public Key Authority (GPKA) and may be found on the GPKA web site, located at:

www.gpka.gov.au

2.7.1 Frequency of entity compliance audit

The RCA must conduct a comprehensive compliance audit of the practices documented in this CPS:

1. within one year of the commencement of operations of a customer operated CA or RA service, at the sole expense of the customer provided such expense is reasonable in all the circumstances;
2. at any other time that it deems warranted and at its own expense, provided a minimum of one month's notice is given.

2.7.1.1 CA and RA Certificate Renewal Compliance Audit

The RCA conducts general compliance audits of subordinate CAs whenever a CA Certificate is due for renewal, at the sole expense of the CA, provided such expense is reasonable in all the circumstances.

CAPL may endorse an audit conducted by a subordinate CA.

A substantial level of non-compliance with any of the following may result in the RCA rejecting the CA's request for Certificate renewal:

1. Model Services or other Operating Agreement;
2. various CP under which Certificates are issued;
3. this CPS.

CAs conduct general compliance audits of subordinate RAs whenever an RA Certificate is due for renewal, at the sole expense of the RA being audited, provided such expense is reasonable in all the circumstances.

CAPL may endorse an audit conducted by a subordinate RA.

A substantial level of non-compliance with any of the following may result in the CA rejecting the RA's request for Certificate renewal:

1. Model Services or other Operating Agreement;
2. various CP under which Certificates are requested;
3. this CPS.

CAs provide a copy of all audit reports they complete to the RCA. The RCA may use such audit reports:

1. to determine the effectiveness of the audits conducted by an auditing CA;
2. to identify the need to conduct its own CPS compliance audit of the audited RA;
3. for any other purpose that promotes the efficient and trustworthy operation of the PKI, for example to assist in identifying operational trends or systemic deviations.

2.7.2 Identity/qualifications of auditor

The GPKA conducts external audits of CAPL Service Providers.

2.7.3 Auditor's relationship to audited party

Aside from the audit function, the GPKA and the audited Service Provider do not have any current or planned financial, legal, or other relationship that could result in a conflict of interest.

2.7.4 Topics covered by audit

The topics covered by a compliance audit consist of the Gatekeeper evaluation

criteria defined by the Government Public Key Authority (GPKA).

The evaluation criteria includes an audit of:

1. physical security;
2. documentation and process;
3. vetting of operations personnel;
4. technology;
5. privacy, including compliance with Commonwealth Government Information Privacy Principles;
6. financial viability and industry development.

2.7.5 Actions taken as a result of deficiency

Copies of the Audit report are submitted to:

- General Manager - Certificates On-Line
- the GPKA (In – Confidence);
- the audited body.

When irregularities are found, General Manager - Certificates On-Line shall promptly oversee or implement an appropriate corrective action.

2.7.6 Communication of results

Audit results are considered to be sensitive commercial information. Unless otherwise specified in contract, they are protected in accordance with section 2.8.

2.8 Confidentiality and privacy

2.8.1 Types of information to be protected

2.8.1.1 Personal information

For the purposes of this CPS, Personal Information has the same meaning as it has in the Privacy Act 1998 (Cth) (The Act).

The Act specifies 11 Information Privacy Principles which apply to the protection of Personal Information provided to Agencies.

In relation to Personal information that is provided to CAPL, CAPL will comply with the Information Privacy Principles as if they were an Agency of the Commonwealth.

2.8.1.2 Tax File Number information

No tax file number is to be retained, recorded or used in registration records or in any other type of document or record. This information will be protected in accordance

with any relevant legislation.

2.8.1.3 Registration information

All information collected or held by CAPL shall only be used in support of the operations of the CAPL PKI, or in support of a compliant transaction.

Personal Information collected in support of this CP will fall into two categories;

1. by RAs about individual End Entities - Evidence Of Identity information, e.g. registration records;
2. by CAs about individual End Entities and about employees of RAs - Certificate information, e.g. information used to populate a field in an X.509 Certificate.

2.8.1.4 Certificate information

At the time a registration record is created by the RA, information collected includes Personal Information.

Some of this information will, pursuant to the *ITU – T Recommendation X.500 (1993) ISO/IEC 9594 – 1: 1993, Information technology – Open Systems Interconnection – The Directory: Overview of Concepts, Models and Services*, and in accordance with the Distinguished Name conventions approved by the GPKA, needs to be included in the Certificate.

By providing Personal Information to CAPL which CAPL embodies in a Certificate held as part of the Registration Record, and includes in the Certificate in accordance with the previous paragraph, the Subscriber is deemed to have agreed to the use of the Personal Information for this purpose.

All other information concerning the registration record, will be protected as Personal Information in accordance with 2.8.1.1. This provision does not operate to prevent publication of the Certificate information.

2.8.1.5 Confidential information

Some information provided to CAPL will be another entity's confidential information.

Access to confidential information by operational staff is on a need-to-know basis.

Paper-based records and other documentation containing confidential information are kept in secure and locked containers or filing systems, separate from all other records.

2.8.1.6 CAPL documentation

The following CAPL documents are considered to be confidential information of CAPL:

1. CONOPS;
2. Head Agreement or other Operating Agreement;

3. Protective Security Risk Review;
4. System Security Plan;
5. Contingency & Disaster Recovery Plan;
6. Configuration Baseline;
7. Operating Procedures.

2.8.1.7 Other Protected information

Certain information provided to CAPL will be protected under specific legislation, or guidelines made known to CAPL. In relation to this information, CAPL 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

RA's are required to inform potential Subscribers that the information included on the Certificate that identifies the Subscriber will be disclosed and is deemed to be Public knowledge where:

1. the Certificate is used in its intended fashion;
2. the information appears in a Public directory.

2.8.2.2 CAPL documentation

The following CAPL documents are public documents and are not considered to be confidential information:

1. CP;
2. this CPS;
3. Security Policy (Public);
4. Privacy Policy (Public);
5. Certificate Key Management Plan (Public).

2.8.3. Disclosure of Certificate revocation/suspension information

2.8.3.1 Disclosure of Certificate suspension information

Information on Certificate suspension is not disclosed. The Directory provides information indicating the fact of suspension, but not the reason for the suspension status.

2.8.3.2 Disclosure of Certificate revocation information

Certificate revocation information contained in the Certificate Revocation List (CRL) shall be publicly available via the CAPL X.500 Directory.

Note that information leading to a decision to revoke will not be disclosed by CAPL - only the fact of revocation will be disclosed through the CAPL X.500 Directory.

Access to the Directory shall be via a web page on a single search basis.

2.8.4. Release to law enforcement officials

As a general principle, no document or record belonging to or held by the CAPL hierarchy shall be released to law enforcement agencies or officials except where:

1. a properly constituted warrant is produced or the information is otherwise legally required to be disclosed; and,
2. the law enforcement official is properly identified.

Registration records are only releasable to law enforcement agencies and officials of those agencies where:

1. a properly constituted warrant is produced or the information is otherwise legally required to be disclosed; and,
2. the law enforcement official is properly identified.

2.8.5. Release as part of civil discovery

As a general principle, no document or record belonging to or held by the CAPL hierarchy shall be released to any person except where:

1. 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,
2. the person requiring production is a person authorised to do so.

2.8.6. Disclosure upon owner's request

The subject of the registration record shall have full access to that record, and shall be empowered to authorise release of that record to another party. The subject of a registration record will not have access to any other subject's registration record unless proper authorisation is given by the relevant person.

Formal authorisation may take two forms:

1. a properly constituted electronic request providing that the request is digitally signed by a valid digital signature under a recognised CP; or,
2. by application in writing.

No release of information is permitted without a formal authorisation in accordance with this section.

2.8.7. Other information release circumstances

No other release of information is permitted unless authorised by a person the information is about, or unless required by law.

2.9 Intellectual Property rights

Please refer the relevant CP.

2.9.1 General provision

Please refer the relevant CP.

2.9.1.1 CAPL PKI

Please refer the relevant CP.

2.9.1.2 Public and Private Keys

Please refer the relevant CP.

2.9.1.3 Certificate

Please refer the relevant CP.

2.9.1.4 Distinguished names

Please refer the relevant CP.

2.9.2 Copyright

2.9.2.1 General

Please refer the relevant CP.

2.9.2.2 in OID

Please refer the relevant CP.

3. IDENTIFICATION AND AUTHENTICATION

3.0 General

3.0.1 CA and RA initial registration

A fundamental concept underpinning the operation of CAPL's PKI is trust. Trust must be realised in each and every aspect of the service operation. At CAPL's discretion, other trustworthy parties may be permitted to operate CA and RA services within CAPL's chain of trust after they have been accredited by the GPKA.

To ensure the integrity and trustworthiness of operations throughout the PKI hierarchy, customer operated CAs and RAs must agree during registration to comply with the practices in this CPS.

3.0.1.1 Submission of application to operate a CA or RA

An application by a third party to operate a CA and/or RA within the CAPL chain of trust should be made in the form of a letter of request (on organisational letterhead) to:

**General Manager - Certificates On-Line
Certificates Australia Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
2060 AUSTRALIA**

CAPL does not permit private individuals to operate as CA or RA services.

Applications to operate a CA or RA service must include the following details, which may be appended to the letter of request:

1. the legal name of the party making the application;
2. any registered business names or other trading names used by the applicant relevant to the operation of the proposed CA or RA service;
3. the proposed name under which the CA or RA will be operating;
4. the domain name and IP address for CA or RA operations;
5. full contact details as follows:
 - residential and mailing address;
 - telephone and facsimile number(s);
 - e-mail address;

- authorised representatives and their contact details;
 - designated operational/administrative contacts and their contact details;
6. a statement that the applicant:
- has read this CPS;
 - agrees to contractually bind the proposed CA or RA service to the practices prescribed therein; and,
 - consents to be accredited in accordance with the requirements of the GPKA.

3.0.1.2 Consideration of Application

When CAPL receives an application from a third party to operate a CA and/or RA within the CAPL chain of trust:

1. an authorised representative of the applicant attends a registration interview in person. During the interview, the representative produces original copies of EOI documentation totalling a minimum of 100 points in the Gatekeeper EOI schema;
2. the applicant, on acceptance of an application to enter Gatekeeper, or after it has been accredited by the GPKA:
 - submits a Concept of Operations (CONOPS) document for CAPL's approval;
 - enters into a contractual relationship entering into a Model Services or other Operating Agreement;
 - submits the CP under which Certificates will be issued to the CAPL PAA for approval;
3. CAPL approves or rejects the application. CAPL is under no obligation to disclose its reasons, or information considered, in rejecting an application. CAPL reserves the right to revoke its approval if subsequent requirements for the commencement of operations are not met in full or to its satisfaction.

3.0.1.3 Requirements for commencement of operations

If the application to operate CA or RA services is approved, prior to commencement of operations:

1. CAPL advises the new service of its OID and distinguished name;
2. the CAPL RCA provides:
 - CA or RA software and hardware;
3. the new CA or RA establishes under CAPL's auspices, a range of policy, planning and operational documentation including:
 - Protective Security Risk Review;

- System Security Plan;
 - CA or RA Operating Procedures.
4. the new CA or RA generates its own keys, then has its Public Keys certified by the CAPL RCA or the CAPL CA, as the case may be;
 5. all operational procedures are vetted for compliance before they are implemented.

3.0.2 End Entity initial registration

3.0.2.1 Pre-registration interview

End Entities making their initial application for a Certificate under a relevant CP are to be provided with the following information, during a pre-registration interview that may be completed immediately prior to registration:

1. an explanation of the nature, purpose and effect of the relevant CP and this CPS;
2. copies of relevant CP and this CPS, or the web site addresses where they are published;
3. their rights, obligations and duties under the relevant Subscriber agreement;
4. advice of the documentation required for EOI purposes;
5. if applicable, the End Entity's right to generate their own keys;
6. End Entities will be informed of various Certificate types that may be available to them.

The above information may alternatively be provided to End Entities in written form a reasonable time before the registration interview, together with contact information for any questions the End Entity may have.

3.0.2.2 Registration interview

The practices described in this section apply to all End Entities making:

1. their initial application for a Certificate under a relevant CP;
2. any subsequent application for a new Certificate under that CP.

This section does not apply to Certificate renewal, unless otherwise provided for within this CPS or the pertinent CP.

The registration interview is to:

1. be attended by the End Entity in person, in the case of an organisation the registration is to be attended by an authorised representative;
2. be conducted by an authorised RA;
3. perform the following functions:

- collection of Certificate information;
- EOI;
- proof of other material Certificate information;
- completion of a Subscriber agreement;
- completion of a third party relying agreement, if required;
- acceptance of Public Keys generated by the End Entity (if applicable).

Disabled potential Subscribers may use an Agent to assist them to complete the registration process. Customers may arrange with an RA to deliver completed registration information and signed agreements to the RA in accordance with alternative procedures agreed to between CA, RA and customers.

Where the RA generates key pairs for the End Entity, this may be done during the registration interview, or as post-interview processing of the Certificate application.

The End Entity's distinguished name, which is decided by the registrar, may also be confirmed during the interview or determined during post-interview processing.

At the end of the interview, the End Entity is provided with a copy of all forms and other documentation completed, including a copy of the Certificate information, the EOI form, the signed Subscriber agreement and any notes made by the registrar.

The requirement to attend an interview may be suspended, at the approval of the GPKA and/or CAPL PAA (as appropriate).

3.0.2.3 Collection of Certificate information

The information required for the issuing of the requested Certificate is obtained from the End Entity. The End Entity's contact details are additionally obtained at this time. The full information collected typically includes:

1. Certificate type;
2. full name (for individuals);
3. organisation and department (for organisational End Entities);
4. e-mail address;
5. other contact details such as telephone number, facsimile number and mailing address;
6. other information may be required specific to the individual RA's operations and/or the nature of the Certificate usage, for example:
 - billing information such as an organisational cost centre number;
 - attributes that are to be included in an Attribute Certificate;
 - an access control mechanism to identify the user in the event of a telephone request for Certificate revocation.

This information may be collected on a paper-based form (e.g. a Certificate application form) for later processing or entered directly into the RA software.

Registrars are to make reasonable efforts to confirm the accuracy of Certificate information. Individual CP may prescribe specific criteria for the authentication of information critical to Certificate usage, for example:

1. in the event that an End Entity's residential address is considered by a community of interest to be material Certificate information, and is included in Certificates issued under a relevant CP, Registrars may be required to follow a set procedure to verify that address;
2. specific documentation may need to be sighted to verify an organisation's:
 - membership in a chamber of commerce or industry body;
 - compliance with certain standards, for example ISO9000;
 - Australian Business Number (ABN);
 - ASIC company number (if applicable).

3.0.2.4 Proof of Identity

The EOI documentation offered by the End Entity must be original copies that have been issued without alteration or erasure.

The registrar is to:

1. record the EOI documentation they sight on a EOI form that complies with the recommended form published in the CP;
2. in the presence of the End Entity:
 - take a copy of each document and seal those copies in an envelope;
 - attach the EOI form to the front of the envelope.

Specific criteria for EOI are contained in relevant CP.

3.0.2.5 Proof of employment

Where a Certificate verifies a person's employment, or Certificate use is based upon the person's authority as a result of their employment, proof of employment must be obtained during initial registration. Specific criteria for proof of employment are contained in relevant CP.

Proof of employment is typically accomplished by the applicant furnishing a request on organisational letterhead:

1. for the issue of a nominated type of Certificate;
2. signed by an authorised officer whose signature is known to the registrar.

3.0.2.6 Completion of a Subscriber agreement

The Subscriber agreement is to comply with the recommended agreement published in the CP.

Prior to obtaining the End Entity's signature on the agreement, the registrar is to confirm that the End Entity understands their rights, obligations and duties under the agreement as explained during the pre-registration interview. The End Entity may take a copy of the Subscriber agreement and other relevant documentation to seek advice from a solicitor, etc. prior to signing.

The Subscriber agreement must be signed in the presence of the registrar.

3.0.2.7 Acceptance of Public Keys generated by the End Entity

In the event that key pairs have been generated by the End Entity, the RA is to ensure during post-interview processing that the applicant is:

1. in possession of the associated Private Keys, this may typically be accomplished by exchanging digitally signed and encrypted e-mail messages with the applicant; and,
2. the true owner of the key pairs, this may typically be accomplished by:
 - the RA checking, and arranging for any other RAs within the policy domain to check, its records to ensure the Public Keys are not already listed against any current operational or revoked Certificate;
 - additionally, if deemed appropriate, obtaining a statutory declaration to that effect.

The registrar is to additionally determine during post-interview processing, based on the Customer's specifications, that the Public Keys are of the required key length.

The method to prove possession of the Private Key is set out in 3.1.7.

3.0.2.8 Post-Registration interview processing

After the registration interview has been completed, the registrar considers the Certificate application and approves or rejects it.

If the application is approved, the registrar uses the RA software to transmit a digitally signed Certificate request to the issuing CA.

If the application is rejected, the applicant is to be promptly informed. The registrar and the RA are under no obligation to disclose the reason for the rejection of any Certificate application, except where required by the CP under which the Certificate was to have been issued, or by law or government regulation. A person or organisation whose application has been rejected may reapply not less than three months after the date of the application.

3.1 Initial registration

3.1.1 Types of names

All Certificate holders require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

The CAPL RCA approves naming conventions for the creation of distinguished names for Certificate applicants. Different naming conventions may be used in different policy domains.

RAs propose and approve distinguished names for Certificate applicants, and as a minimum check that a proposed distinguished name is unique, verify that the name is not already listed in the CAPL X.500 Directory.

3.1.2 Need for names to be meaningful

Distinguished names must be meaningful. Pseudonymous names may be used in the common name component of a distinguished name where requested by an End Entity, provided the End Entity can satisfactorily establish their right to use the pseudonym.

RAs are not to accept pseudonymous names which they believe may cause offence.

The CAPL PKI supports the use of Certificates as a form of identification within a particular community of interest. Anonymous Certificates are not supported by the CAPL PKI.

3.1.3 Rules for interpreting various name forms

The normal operation of some types of Certificate generation requires the insertion of an organisation name and department as part of the distinguished name.

Where a CP does not require an organisation identifier or department identifier in a Certificate, the following changes are to be made to the distinguished name:

Organisation name	Not Applicable
Department name	Not Applicable

3.1.4 Uniqueness of names

Distinguished names are to be unambiguous and unique.

3.1.5 Name claim dispute resolution procedure

Any dispute regarding a Distinguished Name is resolved in terms of section 2.4.3.2 *Process*.

3.1.6 Recognition, authentication and role of trademarks

Recognition, authentication and the role of trademarks is a commercial issue. Nothing in this CPS shall prevent the use of a trademark in a Distinguished Name.

3.1.7 Method to prove possession of Private Key

The Registrar must satisfy itself that the Private Key in the possession of the End Entity does in fact correspond to the Public Key in the possession of the End Entity.

The method to be employed to do this must be detailed in the RA operating procedures, but should, at the minimum involve signing and verifying a message.

This should be done for both the Authentication keys and the Confidentiality keys.

This may typically be accomplished by exchanging digitally signed and encrypted e-mail messages with the applicant.

The registrar is to also take reasonable steps to ensure the End Entity is the true owner of the key pairs. Reasonable steps might typically consist of:

1. the RA checking, and arranging for any other RAs within the policy domain to check, its records to ensure the Public Keys are not already listed against any current operational or revoked Certificate; and,
2. additionally, if deemed appropriate, obtaining a statutory declaration from the End Entity that they are the true owner of the key pairs.

If any doubt exists, the registrar is not to request certification. If the End Entity's right to use or possession of self-generated keys cannot be shown or proven, or reasonable doubt exists:

1. the applicant's details are to be reported to the CA;
2. the application may be progressed using key pairs generated by the RA.

3.1.8 Authentication of organisation identity

An organisation's identity is to be authenticated:

1. during an interview with an authorised registrar attended in person by an authorised representative of the organisation;
2. in compliance with:
 - the EOI practices described in this CPS;
 - the process and forms described in the relevant CP.

No on line techniques are approved for organisational identification.

3.1.9 Authentication of individual identity

An individual's identity is to be authenticated:

1. during an interview with an authorised registrar attended in person by the individual;
2. in compliance with:
 - the EOI practices described in this CPS;
 - the process and forms described in the relevant CP.

No on line techniques are approved for individual identification.

3.2 Routine Rekey

End Entities may request Certificate renewal provided that:

1. the request is made prior to the expiry of their current Certificates;
2. material Certificate information as contained in registration records has not changed;
3. their current Certificates have not been revoked;
4. their keys are not listed as compromised keys;
5. they are not listed as a compromised user.

If any of these conditions are not met, the End Entity must apply for a new Certificate, providing all information and documentation required at an initial registration interview and signing a new Subscriber agreement.

Certificate renewal is governed by the associated CP. Where a CP provides for on line renewal requests, such requests must be digitally signed by the End Entity. A CP may require on line requests to comply with a prescribed file format, or may allow End Entities to send free-form e-mail messages, etc.

In the event that on line requests are not provided for in a CP or are not possible for particular End Entities, End Entities must attend a Certificate renewal interview in person with an authorised registrar, during which they may be required to produce identification and/or other authentication documentation in compliance with the CP. The End Entity must make a renewal request in writing that is signed in the presence of the registrar, who is to verify the End Entity's signature.

Key pairs must always expire at the same time as the associated Certificate. When an End Entity requests Certificate renewal, they are requesting both new Certificates and new key pairs.

CAs are to verify and process Certificate renewal requests on the day they are received.

3.3 Rekey after Revocation

Rekey is not permitted after Certificate revocation. End Entities requiring a replacement Certificate after revocation must:

1. attend an initial registration interview; and,
2. apply for a new Certificate, complying with all initial registration interview procedures and requirements as though they were a new user.

3.4 Revocation request

A request to revoke keys and Certificates, if initiated by an authorised party and signed by a valid key and Certificate under the relevant CP:

- Shall constitute a valid and enforceable revocation request;

- May be made in writing in the form described at 4.4.3.3.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

It is the responsibility of individuals, organisations and government departments, agencies and authorities requiring keys and Certificates to make that request to an approved RA.

Certificate applicants must choose the type of Certificate they require. Registrars may advise applicants on the functionality, authority levels, security services and other attributes or characteristics of differing Certificate types and may recommend the Certificate type that best suits the applicant's needs. However, the decision to apply for a Certificate is to be made solely by the applicant, and the applicant is to independently assess and determine the appropriateness of any type of Certificate for a specific purpose.

There may be many RAs issuing Certificates for a particular policy domain. These RAs may be differentiated by their geographical proximity to the Certificate applicant, the type of Certificates they are authorised to issue or by their organisational relationship to the Certificate applicant's department.

4.2 Certificate Issuance

RAs and CAs are to take reasonable care in accepting and processing Certificate applications. They are to comply with the practices described in this CPS and with any requirements imposed by the CP under which the Certificate is being issued.

In particular, care should be taken to ensure Certificate information does not contain any factual misrepresentations and that no data entry errors are made when accepting an application or generating a Certificate.

RAs and CAs are responsible for monitoring, inquiring into investigating and confirming the accuracy of Certificate information after a Certificate has been issued. Where advice is received that Certificate information is inaccurate or no longer applicable, the matter is to be referred to the Agency concerned before any action is taken in relation to the Certificate.

4.2.1 Certificate issue process

The Certificate issue process is governed by the CP under which the Certificate is issued. Typically, Certificate issue involves:

1. the End Entity personally attending a registration interview, during which an authorised registrar:
 - obtains the End Entity's registration details and Certificate information;
 - authenticates critical Certificate information such as the user's identity;
 - explains the appropriate CP and this CPS to the user, and the user's

responsibilities attached to possession and use of their Public Keys and Certificates;

- obtains in their presence, the End Entity's signature on a Subscriber agreement;

The requirement to attend an interview may be suspended, at the approval of the GPKA and/or CAPL PAA (as appropriate).

2. the RA generates the Certificate key pairs and provides the End Entity with an associated Personal Identification Code (PIC). The PIC is required to access the keys and Certificates when they are later delivered to the End Entity via a secure transport medium. Note that:
 - some CP may allow key pairs to be generated by the End Entity as well as by the RA in which case, the End Entity must prove possession of the Private Keys corresponding to the Public Keys supplied to the RA, and must establish their right to use the key pairs;
 - the practice of using a PIC is recommended but not mandatory. In certain situations, for example the transport of keys and Certificates in a physically secure environment between trusted parties, a CP may exclude the use of a PIC;
 - some CP may require the PIC to be split into two portions that are delivered to the End Entity by different methods, to mitigate against the risk of the PIC being intercepted by a third party;
3. the registrar processes the End Entity's Certificate application and submits a Certificate request to the issuing CA for each Public Key, together with the Public Keys;
4. the issuing CA receives the Certificate requests and Public Key. On the day of receipt the CA verifies each request, generates and signs the requested Certificate(s), then:
 - posts the Certificate(s) to the CAPL X.500 Directory;
 - issues the Certificate(s) to the RA;
5. the RA sends the End Entity an e-mail message, or advises them by other means, that their keys and Certificates are available. Some CP may require the keys and the Certificates to be attached in a secure format to the e-mail message;
6. the End Entity:
 - installs a recognised End Entity application on their PC;
 - accesses their keys and Certificates in a secure format. The keys and Certificates may be retrieved from a web site, attached to an e-mail message, delivered via removable storage media or accessible on a network drive;
 - uses their PIC to import the keys and Certificates into their End Entity application. During the import process, the End Entity protects the Private Keys being stored on their PC by entering an access control mechanism known only to them;

7. the End Entity's keys and Certificates are now ready for operational use.

4.2.1.1 Relying parties

Relying parties need to access nominated Certificates for the authentication of digital signatures and/or decryption of secured files. They may obtain the Certificates they require directly from Certificate owners, or by requesting Certificates from the CAPL X.500 Directory services.

4.2.1.2 End Entity's consent required

Certificates should not be issued:

1. without an End Entity's consent;
2. through an RA other than where the Certificate application was made.

For the purposes of this CPS, a signed Subscriber agreement is deemed to be the End Entity's specific consent to, and request for the issue of Certificates through the registering RA.

4.2.1.3 CAs' right to reject Certificate requests

Certificates are issued at the discretion of the CA receiving a Certificate request. All CAs have the right to reject a Certificate request. If a Certificate request is rejected, the requesting RA is to promptly inform the applicant. CAs are under no obligation to disclose the reason for the rejection of any Certificate request, except where required by the CP under which the Certificate was to have been issued, or by law or government regulation. A person or organisation whose Certificate request has been rejected may reapply not less than three months after the date of the Certificate application.

4.2.1.4 Operational periods

All Certificates begin their operational period on the date of issue. The operational period of a Certificate is governed by:

1. the Model Services or other agreement;
2. the Certificate Profile;
3. the CP;
4. this CPS.

The expiry date of issued Certificates must not result in an operational period greater than that permitted by the above instruments. In the event that a Certificate is issued with a greater than permitted operational period, the Certificate is to be revoked.

4.3 Certificate Acceptance

An End Entity's receipt of a Certificate, and their subsequent use of their keys and Certificates, constitutes Certificate acceptance.

By accepting a Certificate, the user:

1. agrees to be bound by the continuing responsibilities, obligations and duties imposed on them by their Subscriber agreement, the associated CP and this CPS;
2. warrants that to their knowledge no unauthorised person has had access to the Private Key associated with the Certificate;
3. asserts that the Certificate information they have supplied during their registration interview is truthful and has been accurately and fully published within the Certificate.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

Revocation can be described as no longer being able to use a Certificate. A service provider or End Entity's Certificate is revoked when:

1. the Certificate owner or their keys or Certificates are compromised through:
 - the theft, loss, disclosure, modification, or other compromise or suspected compromise of the user's Private Key(s);
 - the deliberate misuse of keys and Certificates, or a substantial non-observance of operational requirements in the Subscriber agreement or associated CP or of the practices in this CPS;
2. a Certificate owner leaves the CAPL community of interest, for example:
 - an organisational End Entity leaves the employment of their organisation;
 - a service provider ceases operations;
 - the decease of an End Entity;
3. there is an improper or faulty issue of a Certificate due to:
 - a material prerequisite to the issue of the Certificate not being satisfied;
 - a material fact in the Certificate is known or reasonably believed to be false;
 - data entry or other processing errors;
4. an End Entity generates the keys associated with a Certificate and those keys are found to be weak;
5. material Certificate information becomes inaccurate, for example when the owner of:
 - an identity Certificate changes their name;
 - an attribute Certificate obtains increased system privileges;
6. a properly formatted request is received from an End Entity;

7. a validated request is received from an authorised third party, for example:
 - a court order;
 - a request made by a person with power of attorney;
8. the Certificate of a superior RA or CA is revoked;
9. it is known or there is reason to believe a service provider does not possess the financial resources to maintain its Certificate services.

4.4.2 Who can request revocation

Certificate revocation can be initiated by:

1. any service provider who is in the Certificate owner's chain of trust and is in a superior position in that chain;
2. the owner of the Certificate;
3. an authorised third party.

End Entities may request revocation of their Certificates for any reason, or for no reason, and must request revocation under the conditions specified in 4.4.1 - *Circumstances for revocation*.

Service providers may not request the revocation of, or revoke their own Certificates under any conditions other than those described in 4.4.1 - *Circumstances for revocation*.

4.4.2.1 CAs

CAs operating within the CAPL hierarchy must initiate revocation under the conditions described in 4.4.1 - *Circumstances for revocation*.

4.4.2.2 RAs

RAs operating within the CAPL hierarchy must initiate revocation under the conditions described in 4.4.1 - *Circumstances for revocation*.

4.4.2.3 End Entities

End Entities may request the revocation of their own Certificates for any reason, and must make such requests through an authorised RA.

4.4.2.4 Authorised third parties

Authorised third parties may request Certificate revocation through an authorised RA. Such authorised parties include, but are not limited to:

1. authorised officers in an organisational End Entity's organisation, requesting revocation when the End Entity leaves the employment of the organisation, in which case the RA must verify the officer's authorisation and that the request has actually been initiated by that officer;
2. third parties with Power of Attorney, in which case the RA must verify the Power of Attorney and the identity of the relevant person;

3. the executor of a Certificate Owner's estate, in which case the RA must verify the Certificate Owner's decease, and the appointment and identity of the executor;
4. a Court with jurisdiction within the issuing CA's area of operations, in which case the RA must confirm the validity of the court order.

Note that a court order for Certificate revocation may be served directly on an issuing CA.

4.4.3 Procedure for revocation request

The practices involved in processing of a revocation request will vary depending on the identity of the originator. This section describes the practices where revocation is:

1. requested by the End Entity;
2. verified by an RA;
3. processed by a CA.

Where a revocation request is originated by a party other than the End Entity:

1. the practices employed in processing the request will comply to the fullest extent possible with the practices that are described below;
2. the reason for the request must be documented.

4.4.3.1 CA processing

To process a revocation request initiated by an RA, a CA:

1. receives and authenticates the digitally signed request from the RA;
2. prioritises the request according to the revocation response times contained within the relevant CP;
3. revokes the Certificate;
4. adds the Certificate to its CRL in the X.500 Directory;
5. issues a notice containing the Certificate details and the date and time of revocation to the Certificate owner and for organisational users, to the user's organisation. The notice is not to include the reason for revocation.

Note that:

1. revoked Certificates are not deleted from a CA's directory services;
2. CAs may employ additional methods to issue notices of revoked Certificates to their users such as OCSP.

4.4.3.2 RA processing

To process a revocation request initiated by an End Entity, an RA:

1. receives and authenticates the request;

2. ensures the Certificate and Public Key are current;
3. prioritises the request according to the processing times indicated in the relevant CP;
4. if applicable:
 - adds the user's keys to its list of compromised keys;
 - adds the user to its list of compromised users;
5. sends a digitally signed revocation request to the CA.

The RA verification requirements for revocation requests are the same as for Certificate renewal, and because of these requirements such requests must be delivered to the RA either in the form of digitally signed file, or in person. If delivered in person, the request must be signed in the presence of the registrar.

4.4.3.3 Certificate Revocation Request

A Certificate revocation request, whether in paper or electronic (e.g. e-mail) form, is to contain the information illustrated in the example form below.

Certificate Revocation Request	Date : _____
To: <RA NAME> <RA ADDRESS>	
Section 1 – Certificate details (if known)	
Certificate ID:
Certificate serial number:
Certificate type:
Section 2 – Certificate owner details	
Full Name: (For private individuals, show family name last.)
Organisational users only:	
Organisation:
Department:
Section 3 – Reason for revocation *	
.....	
.....	
.....	

4. such other persons as described in the CP.

4.4.7 Procedure for suspension request

A separate procedure for suspension and revocation is available at:

www.certificates-australia.com.au

4.4.8 Limits on suspension period

Suspension shall be no longer than one business day (grace period). The suspension notice on the Certificate shall be removed where the CAPL CA is reasonably satisfied that:

1. the keys or Certificate have not been compromised;
2. the media holding the Private Key is not compromised.

[Notwithstanding the above, Certificate suspension shall be lifted, or the Certificate revoked, on receipt of a formal advice from the Customer.]

4.4.9 CRL issuance frequency

The CRL in the X.500 Directory is updated at the CRL issuance frequency stated in the relevant CP.

4.4.10 CRL checking requirements

Relying parties should regularly check the validity and currency of a Certificate.

CAPL recommends that relying parties should check at least weekly, however where the value, importance or sensitivity of a message, transaction or other file is high, it is recommended that the relying party checks on a per transaction basis.

4.4.11 On-Line revocation/status checking availability

CAPL provides an on line X.500 Directory for verifying the status of Certificates issued within the CAPL PKI.

4.4.12 On-Line revocation checking requirements

Refer to section 4.4.10 - *CRL checking requirements*.

4.4.13 Other forms of revocation advertisements available

Some CP may support other forms of revocation advertisement, such as a locally distributed CRL.

CAPL operated CAs use only the X.500 Directory for CRLs.

4.4.14 Checking requirements for other forms of revocation

advertisements

Where other forms of revocation advertisement are supported, checking requirements are specified in the relevant CP.

4.4.15 Special requirements re key compromise

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

4.5 Security Audit procedures

The CAPL RCA, CAPL CAs and CAPL RA maintain, and all approved CAPL CAs and RAs are obliged under contract to maintain, adequate records and archives of information pertaining to the operation of the Public Key infrastructure.

RCA, ICA, OCA and RA software automatically preserves an audit trail for the three primary states in the Certificate Management Life Cycle (CMLC), i.e. generation, operational use and expiry.

4.5.1 Types of event recorded

The minimum audit records to be kept include all:

1. types of registration records, including records relating to rejected applications;
2. key generation requests, whether or not key generation was successful;
3. Certificate generation requests, whether or not Certificate generation was successful;
4. Certificate issuance records, including CRLs;
5. audit records, including security related events;
6. revocation records.

4.5.2 Frequency of processing log

Audit logs are processed on a daily, weekly, monthly and annual basis.

4.5.3 Retention period for audit log

Audit logs are retained for a minimum of seven years. They are maintained 'on site' for a minimum period of three months and a maximum period of twelve months.

The audit log shall be retained in archives for a minimum period of seven years or such other time (not exceeding ten years) as required to meet the National Archives of Australia (NAA) requirements, and then transferred to the NAA. If at the completion of that term, CAPL is required by a person to keep the audit log on-line CAPL may charge that person a fee for the provision of that service.

4.5.4 Protection of audit log

Audit logs are encrypted using a key and Certificate specifically generated for the purpose.

4.5.5 Audit log backup procedures

Each service provider in the CAPL hierarchy is to establish and maintain a backup procedure for audit logs.

4.5.6 Audit collection system

The CAPL PKI audit collection system is a combination of automated and manual processes performed by the CA or RA operating system, the CA or RA application, and by operational personnel.

Type of event	Collection System	Recorded by
Successful and failed attempts to changes operating system security parameters.	Automatic	Operating system
Application startup and shutdown.	Automatic	Operating system
Successful and failed log-in and log-off attempts.	Automatic	Operating system
Successful and failed attempts to create, modify, or delete system accounts.	Automatic	Operating system
Successful and failed attempts to create, modify or delete authorised system users.	Automatic	Operating system
Successful and failed attempts to request, generate, sign, issue or revoke keys and Certificates.	Automatic	CA or RA software
Successful and failed attempts to create, modify or delete Certificate holder information.	Automatic	RA software
Backup, archiving and restoration.	Automatic and manual	Operating system and operations personnel
System configuration changes.	Manual	Operations personnel
Software and hardware updates.	Manual	Operations personnel
System maintenance.	Manual	Operations personnel
Personnel changes	Manual	Operations personnel

4.5.7 Notification to event-causing subject

Operations personnel notify their security administrator when a process or action causes a critical security event or discrepancy.

4.5.8 Vulnerability assessments

A Protective Security Risk Review (PSRR) has been completed for the entire CAPL hierarchy. This PSRR covers the overarching risks and threats that may impact the Public Key infrastructure.

Individual threat and risk assessments are required at each subordinate entity level e.g. approved CA and RAs.

4.6 Records Archival

Each service providers in the CAPL hierarchy maintains an archive of relevant records described in this policy.

4.6.1 Types of event recorded

The following audit information is recorded and archived by service providers:

1. audit logs;
2. Certificate request information;
3. Certificates, including CRLs generated;
4. Complete back up records;
5. copies of e-mail logs;
6. formal correspondence;
7. Policy and Practice documentation.

4.6.2 Retention period for archive

4.6.2.1 Secure maintenance of keys

In accordance with OECD Guidelines for Cryptographic Policy only Confidentiality keys are archived. The period for archiving Confidentiality keys shall be a minimum period of seven years from the date of generation or such other time (not exceeding ten years) as required to meet the Australian archives requirements. At the completion of that term, the Confidentiality keys are transferred to National Archives of Australia for which a fee shall be charged.

The confidentiality keys are archived securely on a CD ROM.

4.6.2.2 Secure maintenance of Certificate

Certificates are archived for a minimum period of seven years from the date of expiry, unless another period is specified in the relevant CP.

Certificates are archived securely on a CD ROM.

4.6.2.3 Term of archive maintenance

Audit trail information is kept for a minimum period of seven years from the date of

generation, unless another period is specifically required.

Audit logs are archived securely on a CD ROM.

4.6.3 Protection of archive

Archive media is protected either by physical security, or a combination of physical security and cryptographic protection. It is also protected from environmental factors such as temperature, humidity, and magnetism.

4.6.4 Archive backup procedures

Each service provider has established archive back up procedures to ensure and enable complete restoration of current service in the event of a disaster situation.

4.6.5 Requirements for time-stamping of records

A trusted Time Source is available to all CA infrastructure supported under the CAPL infrastructure. The CAPL time source is acquired from the Global Positioning System.

Trusted third party time-stamping is not presently supported.

Nothing in this CPS will operate to prevent an RA or other third party from offering that service outside of this CPS.

4.6.6 Archive collection system

Each service provider is to establish an archive collection system that meets the requirements of this CPS.

4.6.7 Procedures to obtain and verify archive information

The integrity of a service provider's archives are verified:

1. at the time the archive is prepared;
2. annually at the time of a programmed Security Audit;
3. at any other time when a full security audit is required.

4.7 Key changeover

Key changeover is not automatic. Keys expire at the same time as their associated Certificates and, with the exception of the RCA which issues a new Certificate and new keys to itself, all parties within the CAPL PKI are to obtain new keys by making an application for Certificate renewal a minimum of one week prior to Certificate expiry.

Service providers must:

1. ensure that key changeover causes minimal disruption to subordinate service providers and End Entities in their chain of trust;

2. provide End Entities and any subordinate CAs or RAs with a minimum of three months' notice of planned key changeover.

4.8 Compromise and Disaster Recovery

Each CAPL service provider:

1. has established and maintains detailed documentation covering its:
 - Contingency & Disaster Recovery Plan, including key compromise, hardware, software and communications failures, and natural disasters such as fire and flood;
 - Configuration Baseline, including operating software, anti virus software and PKI specific application programs;
 - backup, archiving and offsite storage procedures;
2. provides the above documentation on the request of:
 - the RCA when conducting a CPS practices audit;
 - persons conducting a security or compliance audit;
3. provides appropriate training to all relevant staff in contingency and disaster recovery procedures;
4. at least annually tests its Contingency & Disaster Recovery Plan with the minimum test activity being the full restoration of operational services as follows:
 - the current operational platform is shut down and disconnected from communications links;
 - system operating software, application programs and operational data is restored onto a new hardware platform, solely from backup media and in compliance with the Configuration Baseline;
 - the restored service is connected to the communications links and the correct operation of its Certificate services tested;
 - service operations are resumed using the original operational platform. All files on the hard disk of the test platform are securely deleted;
 - the Contingency & Disaster Recovery Plan is reviewed in the light of the test results.

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

Each service provider has established a configuration baseline plan, and back-up, archiving and response plan to provide data for identifying component failure and subsequent service restoration.

4.8.2 Entity Public Key is revoked

Each service provider has established a key and user compromise plan that addresses the actions to be taken in the event that the RCA or CA Public Key is revoked.

CAs and RAs are to promptly advise the RCA of any compromise or suspected compromise of their Private Keys.

4.8.3 Entity Private Key is compromised

Each service provider has established a key and user compromise plan that addresses the actions to be taken in the event that an End Entity Private Key is compromised.

4.8.4 Secure facility after a natural or other type of disaster

Each service provider manages its backup, archive and offsite storage in accordance with its configuration baseline plan, and back-up, archiving and response plan.

4.8.5 Contingency & Disaster Recovery Plan

The purpose of this plan is to restore core business operations as quickly as practicable when systems operations have been significantly and adversely impacted by fire, strikes, etc.

The plan should acknowledge that any impact on system operations will not cause a direct and immediate operational impact within the PKI of which the service provider is a part. This means that the plan should have the primary goal of reinstating the service provider platform in order to make accessible the logical records kept within the software. Recovery actions approved within the plan should be given a priority that is in keeping with the recovery of other organisational records that do not have a direct and immediate impact on the organisation's operations.

To implement a Contingency & Disaster Recovery Plan, a service provider:

1. identifies an internal owner for the plan;
2. identifies individuals authorised to initiate disaster recovery action;
3. identifies major elements at risk, for example;
 - operational hardware;
 - CA or RA software application;
 - logical records;
 - RA EOI records;
4. identifies criteria that might prompt disaster recovery initiation;
5. implements recommended precautionary measures such as setting up:
 - an Uninterruptable Power Supply;

- power surge protectors;
6. considers secondary precautionary measures that may be required, such as:
 - a second power supply using an alternate power source;
 - a backup site;
 - trained backup staff;
 7. develops recovery actions and timeframes;
 8. prioritises recovery actions from most significant to least significant;
 9. maintains a record of the hardware and software configuration baseline;
 10. maintains records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure, including the intended maximum period that the system is to be down.

To support the disaster recovery plans of associated RAs, CAs will:

1. maintain dedicated hardware specifically for RA disaster recovery support;
2. configure and deliver a new hardware platform to RAs who experience hardware failure.

4.9 CA Termination

4.9.1 Introduction

The function of this section is to identify the circumstances in which a termination of all or part of the CAPL PKI 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:

1. the parties co-operate with each other in minimising any disruption that may be caused; and,
2. the End Entities' capacity to use the Public Key Infrastructure is maintained.

Full details of the rights and obligations of the various participants will be set out in a business continuity plan (Business Continuity Plan) and the contracts between relevant participants. For this reason, the full range of circumstances where it will be necessary to activate the Business Continuity Plan are not set out in this CPS. However, some of the circumstances where activation of the Business Continuity Plan will be necessary, and the sorts of rights and obligations that will be included, are set out below.

The obligations set out in the Business Continuity Plan (and the relevant contracts) must in the relevant circumstance, be undertaken by:

1. the Commonwealth of Australia acting through the Office for Government Online (OGO);
2. the Commonwealth agency receiving the certification products and/or services;

3. CAPL; and,
4. 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 CAPL;

where a party described at (3) or (4) is ceasing to provide products or services to the Commonwealth Agency for any reason including:

5. expiration of the contract;
6. the relevant contract is to be, or has been, terminated for default or for convenience; or,
7. 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. CAPL RCA Programmed Termination

A programmed termination will arise where there is termination by a party for default or for convenience.

In so far as it is required, CAPL shall effect a transfer of Keys and Certificates to another Gatekeeper compliant and GPKA Accredited RCA in the manner agreed with OGO. For the purpose of this section, Keys and Certificates can be taken to mean any set of Keys and Certificates within CAPL's span of control.

If programmed termination is required by CAPL, then:

1. CAPL will:
 - 1.1. give to OGO and any affected Commonwealth agencies 3 months' prior written notice of its intention to terminate its RCA business operations;
 - 1.2. reasonably co-operate with OGO and all relevant Commonwealth agencies in the selection of an appropriate replacement RCA to take over the CAPL RCA business operations;
 - 1.3. transfer the private key of the CAPL RCA to the replacement RCA, in a highly secure and trustworthy manner, which manner will, if required by the GPKA, be approved by the GPKA;
 - 1.4. transfer the CRL and other directories of Certificates issued by the RCA to the replacement RCA, in a highly secure and trustworthy manner, which manner will, if required by the GPKA, be approved by the GPKA;
 - 1.5. immediately after the transfer of the CAPL RCA private key to the replacement RCA, the CAPL RCA will permanently destroy all copies of the CAPL RCA private key in its possession so that the only copy of the CAPL RCA private key that was used to digitally sign the subordinate CA public key Certificates is held by the replacement RCA;
 - 1.6. provide a formal declaration concerning the destruction referred to paragraph 1.5 (above) to the GPKA, OGO, other relevant Commonwealth agencies and the relevant RCA, CA or RA; and

- 1.7. 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 CA public key certificates for each CA within the hierarchy that has been transferred;
2. All relevant Commonwealth agencies will reasonably co-operate with CAPL in the programmed termination of the CAPL RCA business.

4.9.3. CAPL RCA Non-programmed Termination

A non-programmed termination will arise where pursuant to a law (State or Commonwealth) it is illegal for CAPL or the directors of CAPL to continue the business operations of CAPL (e.g. CAPL becomes insolvent).

If the CAPL RCA is required to implement a non-programmed termination of its business operations, then a representative of the CAPL RCA will immediately advise the GPKA and the other members of the CAPL hierarchy in writing or if writing is inappropriate the representative may advise by telephone, that the RCA will be immediately terminating its business operations.

In this case:

1. all affected Commonwealth agencies and other members of the CAPL hierarchy will, with the assistance of the CAPL RCA, co-ordinate and use all reasonable endeavours to facilitate the transfer of the CRL and other directories of Certificates issued by the RCA, and the transfer of the RCA's private key to a GPKA accredited RCA;
2. CAPL or its administrator/controller/liquidator or representative will:
 - 2.1. assist to the highest degree possible in the transfer of the private key of the CAPL RCA to the replacement RCA, in a highly secure and trustworthy manner, which manner will, if required by the GPKA, be approved by the GPKA;
 - 2.2. assist to the highest degree possible in the transfer of the CRL and other directories of CA Certificates issued by the CAPL RCA to the replacement RCA, in a highly secure and trustworthy manner, which manner will, if required by the GPKA, be approved by the GPKA;
 - 2.3. immediately after the transfer of the CAPL RCA private key to the replacement RCA, permanently destroy all copies of the CAPL RCA private key in its possession so that the only copy of the CAPL RCA private key that was used to digitally sign subordinate CA public key Certificates is held by the replacement RCA;
 - 2.4. provide a formal declaration concerning the destruction referred to in paragraph 3.3 to the GPKA, relevant Commonwealth agencies and the relevant RCA, CA or RA;
 - 2.5. 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 Certificates for each CA within the hierarchy that has been transferred.

4.9.4. Non-Commonwealth CA Business Operations Programmed

Termination

A programmed termination will arise where there is termination by a party for default or for convenience. If CAPL receives from a CA that is within the CAPL hierarchy a notice that the relevant CA ('the CA') intends to implement a programmed termination then:

1. CAPL will, with the assistance of the relevant Commonwealth agencies, co-ordinate and use its best endeavours to facilitate the transfer of End Entities Certificates and the transfer of the CA's private key to a GPKA accredited CA;
2. The CA will:
 - 2.1. give to OGO, the relevant Commonwealth agencies and CAPL 3 months prior written notice of its intention to terminate its CA business operations;
 - 2.2. reasonably co-operate with OGO, all other relevant Commonwealth agencies and CAPL in the selection of an appropriate replacement CA to take over the CA business operations;
 - 2.3. transfer the private key of the CA to the replacement CA, in a highly secure and trustworthy manner, which manner will, if required by the GPKA, be approved by the GPKA and if required by CAPL be approved by CAPL;
 - 2.4. transfer the CRL and other directories of Certificates issued by the CA to the replacement CA, in a highly secure and trustworthy manner, which manner will, if required by the GPKA, be approved by the GPKA and if required by CAPL, be approved by CAPL;
 - 2.5. immediately after the transfer of the CA private key to the replacement CA, the CA will permanently destroy all copies of the CA private key in its possession so that the only copy of the subordinate CA private key that was used to digitally sign End Entity public key Certificates is held by the replacement CA;
 - 2.6. the CA will provide a formal declaration concerning the destruction referred to in paragraph 2.5 to the GPKA, OGO, other relevant Commonwealth agencies and the new RCA, and any CA or RA in that RCA's hierarchy;
 - 2.7. 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 End Entity Certificates for each End User within the hierarchy that has been transferred.
3. The Commonwealth Government will reasonably co-operate with CAPL and the CA in the programmed termination of the CA business.

4.9.5. Non-Commonwealth CA Business Operations Non-programmed Termination

A non-programmed termination will arise where, pursuant to a law (State or Commonwealth), it is illegal for CA that is within the CAPL Hierarchy ('the CA'), or the directors of the CA, to continue the business operations of the CA (e.g. the CA becomes insolvent).

If the CA is required to implement a non-programmed termination of its business

operations, then a representative of the CA will immediately advise the GPKA and CAPL in writing or if writing is inappropriate the representative may advise by telephone, that the CA will be immediately terminating its business operations.

In this case:

1. all affected Commonwealth agencies and CAPL will, with the assistance of the CA, co-ordinate and use all reasonable endeavours to facilitate the transfer of the CRL and other directories of Certificates issued by the CA, and the transfer of the CA's private key to a GPKA accredited CA;
2. the CA or its administrator/controller/liquidator or representative will:
 - 2.1. assist to the highest degree possible in the transfer of the private key of the CA to the replacement CA, in a highly secure and trustworthy manner, which manner will, if required by the GPKA, be approved by the GPKA or if required by CAPL be approved by CAPL;
 - 2.2. assist to the highest degree possible in the transfer of the CRL and other directories of Certificates issued by the CA to the replacement CA, in a highly secure and trustworthy manner, which manner will, if required by the GPKA, be approved by the GPKA or if required by CAPL, be approved by CAPL;
 - 2.3. immediately after the transfer of the CA private key to the replacement CA, the CA will permanently destroy all copies of the CA private key in its possession so that the only copy of the CA private key that was used to digitally sign End Entity Certificates is held by the replacement CA;
 - 2.4. provide a formal declaration concerning the destruction referred to in paragraph 2.3 to the GPKA, CAPL and the relevant RCA or RA.
 - 2.5. use its/their reasonable endeavours to cause the replacement CA within a reasonable time after the date on which the transfer is effected to re-issue End Entity Certificates for each End Entity within the hierarchy that has been transferred.

4.9.6. Non-Commonwealth RA business operations Programmed Termination

A programmed termination will arise where there is a termination by a party for default or for convenience. If a non-Commonwealth RA that is within the CAPL RCA Hierarchy intends to implement a programmed termination then:

1. the RA must give not less than 3 months notice in writing to OGO the CAPL RCA and the CA for which it registers End Entities, of its intention to terminate its business operations in a programmed manner; and
2. CAPL will with the assistance of the relevant CA use its best endeavours to facilitate the transfer in a secure and trustworthy manner of all records held by the RA to a replacement RA. All parties involved in the transfer of the RA records will adhere to the Information Privacy Principles set out in the Privacy Act 1988 (Cth)..

4.9.7. Non-Commonwealth RA business operations Non-

programmed Termination

A non - programmed termination will arise where pursuant to a law (State or Commonwealth) it is illegal for the RA or the directors of the RA to continue the business operations of the RA (e.g. if the RA becomes insolvent).

CAPL will promptly with the assistance of the relevant CA use its best endeavours to facilitate the transfer in a secure and trustworthy manner of all records held by the RA to a replacement RA or if no replacement RA can be promptly located then the relevant subordinate CA will accept the transfer of the RA records that contain the private information concerning the End Entities. All parties involved in the transfer of the RA records will adhere to the Information Privacy Principles set out in the Privacy Act 1988 (Cth).

Where the Directory and associated CRL of Certificates have been transferred to another RCA or CA in accordance with this section 4.9 Subscribers will accept those Certificates as being properly issued by that new RCA or CA as the case may be.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

The site location of the CAPL RCA is in a secure office environment at Level 5, 1 James Place, North Sydney NSW Australia.

The RCA operates within a secure physical environment within the office area that meets the standards required by ACSI 33 CR2.

5.1.2 Physical access

CAPL permits entry to its secure operating area only to authorised personnel, and to visitors under the constant supervision of an authorised person. The number of personnel authorised to enter the area is kept to a minimum and a log is maintained of all accesses.

5.1.3 Power and air conditioning

The RCA secure operating area is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

The area has an air conditioning system to control the heat and humidity that is independent of the building air conditioning system.

5.1.4 Water exposures

The RCA secure operating area is protected against water exposure by being located on an above ground floor of an office building that is not in a flood zone, and having a built-in six inch raised floor.

All critical components are further protected against water exposure by being contained within waterproof cabinets.

5.1.5 Fire prevention and protection

Suitable fire extinguishers are maintained in the RCA secure operating area, to guard against the possibility of fire.

5.1.6 Media storage

All magnetic media containing RCA information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located either within the RCA service operations area or in a secure off-site storage area.

5.1.7 Waste disposal

Paper documents and magnetic media containing the RCA Private Key or commercially sensitive or confidential information are securely disposed of by:

1. in the case of magnetic media:
 - physical damage to, or complete destruction of the asset;
 - the use of an approved utility to wipe or overwrite magnetic media;
2. in the case of printed material, shredding, or destruction by an approved service.

5.1.8 Off-site backup

Endorsed off site storage agents are used for the storage and retention of backup software and data.

The off site storage:

1. is available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data;
2. has appropriate levels of physical security in place.

5.2 Procedural Controls

5.2.1 Trusted roles

In order to ensure that one person acting alone cannot circumvent the entire system, responsibilities at an RCA service workstation are shared by multiple roles and individuals. Oversight may be in the form of a person who is not directly involved in issuing Certificates examining system records or audit logs to ensure that other persons have acted within the realms of their responsibilities and within the stated security policy.

This is accomplished by creating separate roles and accounts on the RCA service workstation, each of which has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. At a minimum, the following roles are established:

1. System Administrator;
2. Registrar (RAs only);
3. Security Administrator.

5.2.2 Number of persons required per task

Separate individuals fill each of the three roles described above. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation. However:

1. a single individual may assume the roles of the System Administrator and Registrar;
2. the Security Administrator must always remain separate from the System Administrator in order to provide an independent review of the audit log;
3. any task requiring the creation, backup or importation into a database of a service provider Private Key must involve two trusted persons, one performing the function and the second fulfilling a security monitoring role.

5.2.3 Identification and authentication for each role

Persons filling trusted roles must undergo a formal vetting process conducted by the Australian Security Vetting Service, designated “Position of Trust”.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The recruitment and selection practices for RCA services personnel take into account the background, qualifications, experience and clearance requirements of each position, which are compared against the profiles of potential candidates.

5.3.2 Background check procedures

Background checks are conducted by the Australian Security Vetting Service on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

5.3.3 Training requirements

All RCA services personnel staff are trained in:

1. basic PKI concepts;
2. the use and operation of the RCA software;
3. documented RCA procedures;
4. computer security awareness and procedures;
5. how to explain to CA Certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
6. the meaning and effect of this CP, and a relevant CPS.

5.3.4 Retraining frequency and requirements

RCA services personnel staff receive a security briefing update at least once a year.

Training in the use and operation of the RCA software is provided when new versions of the software are installed.

Remedial training is completed when recommended by audit comments.

5.3.5 Job rotation frequency and sequence

The RCA may implement formal job rotation practices (e.g. through formal reliefs). Where formal job rotation is not implemented, cross-training activities are conducted to ensure operations continuity.

5.3.6 Sanctions for unauthorised actions

Unauthorised actions by RCA services personnel staff are submitted to staff members with the appropriate authority including, but not limited to, the Security Administrator.

5.3.7 Contracting personnel requirements

RCA services personnel may be contractors who are appointed in writing and given written notification of the terms and conditions of their position. They are normally assigned full-time to their responsibilities.

5.3.8 Documentation supplied to personnel

RCA services personnel have access to all relevant:

1. hardware and software documentation;
2. policy documents, including this CP;
3. operational practice and procedural documents, including a relevant CPS .

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

For more information on Key Pair generation and installation, refer the Key Management Plan and the relevant CP.

6.1.1 Key pair generation

RCA key pairs are generated and installed by the RCA.

6.1.2 Private Key delivery to entity

The self-generated RCA Private Keys do not require delivery.

6.1.3 Public Key delivery to Certificate issuer

The self-generated RCA Public Keys do not require delivery.

6.1.4 CA Public Key delivery to users

The self-generated RCA Public Keys do not require delivery.

6.1.5 Key sizes

The RCA key lengths are determined by a relevant Certificate Profile.

6.1.6 Public Key parameters generation

The parameters used to create Public Keys are generated by the RCA.

6.1.7 Parameter quality checking

The quality of Public Key parameters is automatically checked by the RCA software.

6.1.8 Hardware/software key generation

RCA key generation is performed in hardware or software as prescribed by security policy.

6.1.9 Key usage purposes

Keys may be used for the purposes and in the manner described in Section 1.3.4 *Applicability*.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

Cryptographic modules that may be in use from time to time as part of the operations of the RCA comply with industry standards.

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

Private Keys are not under n out of m multi-person control.

6.2.3 Private Key escrow

Private Key escrow is not supported.

6.2.4 Private Key backup

The RCA Private Key is stored in an encrypted database, which is backed up under further encryption with backup copies maintained on site and in secure off site storage.

6.2.5 Private Key archival

See section 4.6.2.1 *Secure maintenance of keys*.

6.2.6 Private Key entry into cryptographic module

Where a cryptographic module is used, the Private Key must be generated in it and remain there in encrypted form, and be decrypted only at the time at which it is being used.

6.2.7 Method of activating Private Key

Private Keys are activated by the RCA software, following the successful completion of a login process that requests and validates an authorised user access control mechanism.

6.2.8 Method of deactivating Private Key

Private Keys are de-activated when the RCA software application is terminated.

6.2.9 Method of destroying Private Key

The RCA software destroys Private Keys in memory by overwriting them with zeros when the software shuts down.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key archival

The RCA archives its Public Key.

6.3.2 Usage periods for the public and Private Keys

The usage period for the RCA private and Public Key is ten years.

6.4 Activation Data

6.4.1 Activation data generation and installation

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

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

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

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The RCA has established a System Security Plan that incorporates computer security technical requirements for the operation of the RCA.

6.5.2 Computer security rating

The RCA has established a System Security Plan that incorporates computer security ratings for the operation of the RCA.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

RCA operational software is developed in a controlled environment employing appropriate quality controls.

6.6.2 Security management controls

System security management is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in section 5.2.1 *Trusted roles*.

6.6.3 Life cycle security ratings

The RCA has established a Protective Security Risk Review that identifies and addresses all high or significant life cycle security threats.

6.7 Network Security Controls

The RCA has established a Protective Security Risk Review that identifies and addresses all high or significant network security threats.

6.8 Cryptographic Module Engineering Controls

The RCA has established a Protective Security Risk Review that identifies and addresses all high or significant cryptographic module engineering security threats.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

The RCA supports and uses X.509 Version 3 Certificates, which contain v.3 in the version field.

7.1.2 Certificate extensions

The RCA supports and uses X.509 Version 3 Certificate extensions.

7.1.3 Algorithm object identifiers

OIDs are not allocated to algorithms supported and used within the CAPL PKI.

The following hashing/digest algorithms are supported:

1. Secure Hash Algorithm-1 (SH“-1)
2. Message Digest 5 (“D5”)

The following padding algorithms are supported:

1. ISO “796
2. PK“S#1”
1. The following encryption algorithms are supported:“RSA
2. DES

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

7.1.4 Name forms

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

7.1.5 Name constraints

Anonymous names are not supported. Pseudonymous names that may cause offence are not permitted.

7.1.6 Certificate policy Object Identifier

OIDs are carried in the standard extension field of X.509 Certificates and are published in the CP.

7.1.7 Usage of Policy Constraints extension

The RCA supports the use of the Policy Constraints extension.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate policy extension

See section 1.1.2.1 *X.509 Certificate extensions*.

7.2 CRL Profile

7.2.1 Version number(s)

The RCA supports and uses X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

The RCA supports and uses X.509 Version 2 CRL entry extensions.

8. SPECIFICATION ADMINISTRATION

CAPL operates a Policy Approval Authority which is responsible for setting Certificate policy direction for the overall Public Key infrastructure. Contact details for the PAA appear in each CP applicable to the CAPL hierarchy.

A Policy Creation Authority is normally vested at the CA or equivalent level in a PKI hierarchy. In the case of the CAPL PKI, the PAA and PCA functions are vested in the same authority, the PAA.

Each CP used under the CAPL hierarchy has been allocated an OID which:

1. provides a unique identification for the CP;
2. includes a policy version number.

8.1 Specification change procedures

8.1.0.1 Initial publication

The PAA is the responsible authority for changes to a CP. New CAs apply to the PAA for:

1. formal endorsement of the CP under which they will issue Certificates;
2. the allocation of an OID.

After the CP has been approved and the OID has been granted, the CA:

1. publishes, on a nominated web site, the CP together with this CPS;
2. advises all subordinate parties of the CP and its applicability;
3. forwards a copy of the CP to each subordinate RA, together with an advice regarding the web site of the master CP.

8.1.1 Change

There are two possible types of policy change:

1. the issue of a new CP;
2. a change to or alteration of an existing policy.

If an existing policy requires re-issue, the change process employed is the same as for as for initial publication, as described above. Note that the new OID issued for a policy change differs from the previous OID only in the policy version number.

8.2 Publication and notification policies

New or amended CP are published on the web site nominated in the CP.

Subordinate parties are notified by the appropriate CA of changes to a CP as and when they are approved. Subordinate CAs and RAs are advised of the changes a minimum of one week prior to publication.

8.3 CPS approval procedures

CP intended for use under the CAPL RCA must be endorsed by the CAPL PAA. A document setting out the functions of the CAPL RCA PAA is made available to all subordinate parties responsible for creating or amending CP, the document is also made available to any approved person conducting a security audit.

Appendix A – CP Supported under this CPS

The following CP are supported under this CPS:

1. CAPL RCA CP;
2. CAPL CA CP;
3. CAPL Demonstration CA (DCA) CP;
4. CAPL Gatekeeper - Individual (Type 1 Grade 1) Certificates;
5. CAPL Gatekeeper – Organisation (Type 2 Grade 1) Certificates;
6. CAPL Gatekeeper – Employee (Type 3 Grade 1) Certificates (proposed).