
CAPL RCA Certificate Policy

Document details

Document Serial No.: Obtain next sequential number from P:/DocControl/document.xls
Document Version No.: 2.7
Template: CAPL template.dot
File name: F:\CAPL\Gatekeeper\CAPL - CP IN - (RC - CP) V2.7.Doc
File size: 1772032 bytes
Date printed: 23/01/01 11:41
Date saved: 16/01/01 17:46
Number of pages: 58
Comments: The fields in this document must be updated before printing.



Baltimore Certificates Australia Pty Limited

CAPL RCA Certificate Policy

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 Baltimore Technologies Pty Ltd.

Copyright © 2000 Baltimore Certificates Australia Pty Limited
All Rights Reserved.

The information contained in this document is intended for Baltimore Technologies personnel charged with the management and operation of the Certificate Authorities owned and operated as Baltimore Certificates Australia Pty Ltd or Security Domain Pty Ltd (Baltimore Certificates On Line), those persons named as recipients or those persons nominated in the circulation list.

It may contain privileged and confidential information and if you are not the intended recipient, you must not copy, distribute or take any action in reliance on it.

If you have received this document in error, please notify the author immediately by reverse charge telephone call and return the original to the sender by mail. You will be reimbursed for postage.

Contact:

General Manager – Baltimore Certificates Australia Pty Limited
Level 6, 1 James Place
NORTH SYDNEY NSW 2060
AUSTRALIA

Version history

Doc. Version	Status	Date of Issue	Issued By	Comments
0.1	Draft	16/12/98		Initial Draft
1.0	Final	05/01/99		Signed off by Gadens
1.1	Draft	15/02/99	NJM	Incorporates all IETF PKIX framework 4 headings.
1.2	Final	26/02/99	NJM	Incorporates AGS comments.
2.0	Final	26/09/00	TAS	Incorporate NOIE comments on level 1 type 1 ee cp
2.1	In evaluation	31/10/00	TAS	Incorporates comments from AGS, NOIE, DSD
2.2	In evaluation	31/10/00	TAS, SGL	Incorporates further comments from AGS, NOIE, DSD
2.3	In	8/11/00	SGL	Incorporates further comments from

	evaluation			AGS and NOIE
2.4	In evaluation	9/11/00	SGL	Minor change to one document reference and fixed logo.
2.5	In evaluation	10/11/00	SGL	Changed OIDs to new schema. Multiple minor edits.
2.6	In evaluation	22/12/00	SGL	Removal of references to non-Gatekeeper CAs, minor edits.
2.7	Definitive	17/01/01	SGL	Addressed comments arising from Health OCA incorporation.

Table of Contents

1.	Introduction.....	2
1.1	Overview	2
	1.1.1 Standards	2
	1.1.2 Definitions	2
	1.1.3 X.500 Object Identifier hierarchy.....	3
	1.1.4 Policy Qualifier	3
1.2	Identification	3
	1.2.1 CAPL RCA OID.....	3
	1.2.2 CAPL RCA CP OID.....	3
1.3	Community and Applicability.....	4
	1.3.0 Policy Authorities.....	4
	1.3.1 Certification authorities.....	5
	1.3.2 Registration authorities	7
	1.3.3 Subscribers	8
	1.3.4 Applicability	8
1.4	Contact Details	8
	1.4.1 Specific administration organisation.....	8
	1.4.2 Contact person	8
	1.4.3 Person determining CPS suitability for this policy	8
2.	General Provisions.....	9
2.1	Obligations	9
	2.1.0 CAPL Obligations.....	9
	2.1.1 CAPL RCA Obligations	10
	2.1.2 RA obligations.....	10
	2.1.3 Subscriber obligations.....	10
	2.1.4 Relying party obligations	11
	2.1.5 Repository Obligations	11
2.2	Liability	11
	2.2.0 CAPL liability.....	11
	2.2.1 CA Liability	11
	2.2.2 RA Liability.....	11
	2.2.3 End Entity Liability	12
	2.2.4 Liability of the Commonwealth.....	12
2.3	Financial responsibility	12
	2.3.1 Indemnification by relying parties.....	12
	2.3.2 Fiduciary relationships.....	12
	2.3.3 Administrative processes	12
	2.3.4 Baltimore Certificates Australia Pty Limited.....	13
	2.3.5 Client managed CA and RA services.....	13
2.4	Interpretation and Enforcement	13
	2.4.1 Governing Law	13

2.4.2	Severability, survival, merger, notice, assignment	14
2.4.3	Dispute resolution procedures	15
2.5	Fees	17
2.5.1	Certificate issuance or renewal fees	17
2.5.2	Certificate access fees	17
2.5.3	Revocation or status information access fees	17
2.5.4	Fees for other services such as policy information	17
2.5.5	Refund policy	17
2.6	Publication and repository	17
2.6.1	Publication of RCA information	17
2.6.2	Frequency of publication	18
2.6.3	Access controls	18
2.6.4	Repositories	18
2.7	Compliance Audit	20
2.7.0	Gatekeeper Evaluation	20
2.7.1	Frequency of entity compliance audit	20
2.7.2	Identity/qualifications of auditor	20
2.7.3	Auditor's relationship to audited party	21
2.7.4	Topics covered by audit	21
2.7.5	Actions taken as a result of deficiency	21
2.7.6	Communication of results	21
2.8	Data protection and privacy	21
2.8.1	Types of information to be protected	21
2.8.2	Types of information that may be disclosed	22
2.8.3	Disclosure of Certificate revocation/suspension information	22
2.8.4	Release to law enforcement officials	23
2.8.5	Release as part of civil discovery	23
2.8.6	Disclosure upon owner's request	23
2.8.7	Other information release circumstances	23
2.9	Intellectual Property Rights	24
2.9.1	General provision	24
2.9.2	Copyright	24
3.	Identification and Authentication	25
3.1	Initial registration	25
3.1.1	Types of names	25
3.1.2	Need for names to be meaningful	25
3.1.3	Rules for interpreting various name forms	25
3.1.4	Uniqueness of names	25
3.1.5	Name claim dispute resolution procedure	26
3.1.6	Recognition, authentication and role of trademarks	26
3.1.7	Method to prove possession of Private Key	26
3.1.8	Authentication of organisation identity	26
3.1.9	Authentication of individual identity	26
3.2	Routine Re-key	26
3.2.1	RCA Routine Re-key	26
3.3	Re-key after Revocation	26

3.4	Revocation request	26
4.	OPERATIONAL REQUIREMENTS	27
4.1	Certificate Application	27
4.2	Certificate Issuance	27
	4.2.1 Certificate issue process	27
4.3	Certificate acceptance	27
4.4	Certificate suspension and revocation	28
	4.4.1 Circumstances for revocation	28
	4.4.2 Who can request revocation	28
	4.4.3 Procedure for revocation request	29
	4.4.4 Revocation request grace period	29
	4.4.5 Circumstances for suspension	29
	4.4.6 Who can request suspension	29
	4.4.7 Procedures relating to suspension	29
	4.4.8 Limits on suspension period	30
	4.4.9 CRL issuance frequency	30
	4.4.10 CRL checking requirements	30
	4.4.11 On-Line revocation/status checking availability	30
	4.4.12 On Line revocation checking requirements	30
	4.4.13 Other forms of revocation advertisements available	30
	4.4.14 Checking requirements for other forms of revocation advertisements	31
	4.4.15 Special requirements re key compromise	31
4.5	Security Audit procedures	31
	4.5.1 Types of events recorded	31
	4.5.2 Frequency of processing log	31
	4.5.3 Retention period for audit log	31
	4.5.4 Protection of audit log	32
	4.5.5 Audit log backup procedures	32
	4.5.6 Audit collection system	32
	4.5.7 Notification to event-causing subject	32
	4.5.8 Vulnerability Assessments	32
4.6	Records Archival	32
	4.6.1 Types of events recorded	32
	4.6.2 Retention period for archive	33
	4.6.3 Protection of archive	33
	4.6.4 Archive backup procedures	33
	4.6.5 Requirements for time-stamping of records	33
	4.6.6 Archive collection system	33
	4.6.7 Procedures to obtain and verify archive information	34
4.7	Key changeover	34
4.8	Compromise and Disaster Recovery	34
	4.8.1 Computing resources, software, and/or data are corrupted	34
	4.8.2 Entity Public Key is revoked	34
	4.8.3 Entity Private Key is compromised	35
	4.8.4 Secure facility after a natural or other type of disaster	35
	4.8.5 Contingency & Disaster Recovery Plan	35

4.9	RCA termination.....	35
4.9.1	Introduction	35
4.9.2	CAPL RCA Programmed Termination	36
4.9.3	CAPL RCA Non-programmed Termination	37
4.9.4	Transfer of Root CA Data	38
5.	Physical, procedural, and personnel security controls	39
5.1	Physical Controls	39
5.1.1	Site location and construction.....	39
5.1.2	Physical access	39
5.1.3	Power and air conditioning	39
5.1.4	Water exposures	39
5.1.5	Fire prevention and protection	39
5.1.6	Media storage.....	40
5.1.7	Waste disposal	40
5.1.8	Off-site backup	40
5.2	Procedural Controls.....	40
5.2.1	Trusted roles	40
5.2.2	Number of persons required per task	41
5.2.3	Identification and authentication for each role.....	41
5.3	Personnel Controls	41
5.3.1	Background, qualifications, experience, and clearance requirements	41
5.3.2	Background check procedures	41
5.3.3	Training requirements	42
5.3.4	Retraining frequency and requirements	42
5.3.5	Job rotation frequency and sequence	42
5.3.6	Sanctions for unauthorised actions	42
5.3.7	Contracting personnel requirements.....	42
5.3.8	Documentation supplied to personnel	42
6.	Technical Security Controls.....	43
6.1	Key Pair Generation	43
6.1.1	Key pair generation	43
6.1.2	Private Key delivery to entity.....	43
6.1.3	Public Key delivery to certificate issuer	43
6.1.4	CA Public Key delivery to users	43
6.1.5	Key sizes	43
6.1.6	Public Key parameters generation	43
6.1.7	Parameter quality checking	43
6.1.8	Hardware/software Key generation	43
6.1.9	Key usage purposes	43
6.2	Private Key Protection.....	44
6.2.1	Standards for cryptographic module	44
6.2.2	Private Key (n out of m) multi-person control	44
6.2.3	Private Key escrow	44
6.2.4	Private Key backup.....	44
6.2.5	Private Key archival	44
6.2.6	Private Key entry into cryptographic module	44
6.2.7	Method of activating Private Key	44

6.2.8	Method of deactivating Private Key.....	44
6.2.9	Method of destroying Private Key	44
6.3	Other Aspects of Key Pair Management.....	45
6.3.1	Public Key archival	45
6.3.2	Usage periods for the Public Keys and Private Keys.....	45
6.4	Activation Data	45
6.4.1	Activation data generation and installation.....	45
6.4.2	Activation data protection	45
6.4.3	Other aspects of activation data	45
6.5	Computer Security Controls.....	45
6.5.1	Specific computer security technical requirements.....	45
6.5.2	Computer security rating	45
6.6	Life Cycle Technical Controls	46
6.6.1	System development controls	46
6.6.2	Security management controls	46
6.6.3	Life cycle security ratings	46
6.7	Network security controls	46
6.8	Cryptographic module engineering controls	46
7.	Certificate and CRL Profiles	47
7.1	RCA Certificate Profile	47
7.1.1	Version number(s).....	47
7.1.2	Certificate extensions	47
7.1.3	Algorithm object identifiers	47
7.1.4	Name forms.....	48
7.1.5	Name constraints.....	48
7.1.6	Certificate policy Object Identifier.....	48
7.1.7	Usage of Policy Constraints extension.....	48
7.1.8	Policy qualifiers syntax and semantics.....	48
7.1.9	Processing semantics for the critical certificate policy extension	48
7.2	CRL Profile	48
7.2.1	Version number(s).....	48
7.2.2	CRL and CRL entry extensions.....	48
8.	Specification Administration	49
8.1	Specification change procedures	49
8.1.1	Initial publication	49
8.1.2	Change	49
8.2	Publication and notification policies.....	50
8.3	CP approval procedures	50

1. Introduction

1.1 Overview

This Certificate Policy (“CP”) has been written expressly to comply with the Australian Commonwealth Government’s Gatekeeper strategy for public key technology use in the Commonwealth government.

This CP relates to the self-signed Baltimore Certificates Australia Pty Limited (“CAPL”) Root Certification Authority (“RCA”) Certificate and the Certificates issued for use by its associated administrative interface, known as the Certification Authority Operator (“CAO”).

The CAPL RCA is the highest point of trust within the CAPL Public Key Infrastructure (“PKI”) hierarchy (“CAPL PKI Hierarchy”) on which all other elements and entities in the PKI rely.

The CAPL RCA signs the Certificates of Subordinate CAs operating within the CAPL PKI Hierarchy.

1.1.1 Standards

This CP is based on RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, IETF PKIX RFC2527, by S. Chokhani and W. Ford, March 1999. However, in some instances, this guideline does not provide adequate definition. In such cases, this CP will differ from the guideline insofar as is necessary for clarity only.

1.1.1.1 Certificate types issued

The CAPL RCA shall issue:

1. the self-signed RCA Certificate;
2. CAO Certificates, which are used to operate the CAO software and submit certification and revocation requests to the CAPL RCA;
3. Subordinate CA Certificates (either for Intermediate Certification Authorities (“ICAs”) or Organisation Certification Authorities (“OCAs”)), which must be Gatekeeper accredited;
4. such other Certificates as might be approved by the CAPL Policy Approval Authority (“PAA”).

1.1.2 Definitions

The definitions used within this document are published by CAPL at:

<http://www.certificates-australia.com.au>

These definitions are based on:

- ISO Glossary of IT Security Technology¹; and
- Gatekeeper Glossary of Terms².

1.1.3 X.500 Object Identifier hierarchy

Specified elements under this PKI have been assigned an X.500 Object Identifier (“OID”). The authority for issuing such object identifiers is the CAPL PAA.

1.1.4 Policy Qualifier

The RCA Certificate carries within it a ‘policy qualifier’, which summarises the major points of this CP. The purpose of the policy qualifier is to provide the person relying upon the Certificate with an abbreviated description of the main features of the CP under which the Certificate was issued.

Other fields in the Certificate provide details of where and how to find a complete copy of this CP.

1.1.4.1 Policy Qualifier – RCA

The text of the policy qualifier in the CAPL RCA Certificate is:

“Certificates issued under this policy are self-signed and are issued by the RCA itself.”

1.2 Identification

1.2.1 CAPL RCA OID

The OID for the CAPL RCA is:

1.2.36.75878867.4

1.2.2 CAPL RCA CP OID

The OID for this policy is:

1.2.36.75878867.4.1

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

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

1.3 Community and Applicability

The CAPL RCA Certificate is the highest point in the chain of trust within the CAPL PKI Hierarchy on which all entities in the hierarchy ultimately rely. The CAPL RCA Certificate is used by Relying Parties to establish this chain of trust.

This CP is applicable to:

1. the CAPL RCA; and
2. the CAPL RCA CAO (the Administrative interface into the CAPL RCA); and
3. the Subordinate CAs whose Certificates are issued by the CAPL RCA.

1.3.0 Policy Authorities

Three policy approval authorities are relevant to this CP:

- the National Office for the Information Economy (“NOIE”)
- the CAPL Policy Approval Authority (“PAA”)
- the Policy Management Authorities (“PMAs”)

1.3.0.1 National Office for the Information Economy (NOIE)

NOIE is responsible for defining the high level criteria against which Certification Authorities and Registration Authorities are to be evaluated and, when successfully evaluated, Gatekeeper accredited. Once accredited, an OCA may offer and issue Certificates to Commonwealth agencies or to those organisations and entities with which the agencies conduct electronic transactions.

1.3.0.1.1 NOIE Contact details

The contact details for the CEO, NOIE are:

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

1.3.0.2 CAPL Policy Approval Authority (CAPL PAA)

The CAPL PAA sets out the overarching operational doctrine for the CAPL PKI Hierarchy.

The CAPL PAA has the following functions:

1. to approve CPs within the CAPL PKI Hierarchy;
2. to approve the creation of a new CAPL RCA Certificate;
3. to approve the establishment of PMAs;
4. to administer subordinate policy infrastructure to maintain the integrity of the PKI.

1.3.0.2.1 CAPL PAA Contact details

The contact details for the CAPL PAA are:

Name:	Baltimore Certificates Australia Pty Limited
Contact:	Policy Approval Authority
Title:	General Manager – BCAPL
ACN:	075878867
Trading as:	CAPL
Postal Address:	Level 5, 1 James Place North Sydney NSW 2060 Australia
Phone:	+61 2 9409 0300
Fax:	+61 2 9409 0301
E-mail Address:	info@certificates-australia.com.au

1.3.0.3 Policy Management Authorities (PMA)

The PMAs are responsible for the creation of policy unique to the operation of a particular CA.

A PMA performs the following functions:

1. formulates new policy and policy changes within the CAPL PKI Hierarchy;
2. submits new or changed policies to the CAPL PAA for approval.

1.3.1 Certification authorities

1.3.1.1 CAPL RCA

The registered address of the CAPL RCA is:

Baltimore Certificates Australia Pty Limited Level 5, 1 James Place NORTH SYDNEY NSW 2060 AUSTRALIA
--

1.3.1.2 CAPL RCA Functions

The functions performed by the CAPL RCA are:

1. constitution of a PAA for the purposes of reviewing and approving policies applicable to, and recognised by, the CAPL RCA;
2. generation of its own Keys using software that is listed on the DSD's Evaluated Products List ("EPL");
3. issuing of a self-signed Certificate;
4. publication of the CAPL RCA's Public Key Certificate in the CAPL X.500 Directory;
5. provision to Relying Parties of access to:
 - Certificate information published in the CAPL X.500 Directory;
 - the Public Keys associated with operational Certificates that are listed in the CAPL X.500 Directory;
6. publication of the CAPL RCA Hash on the CAPL Websites ("CAPL Websites") at:

<http://www.certificates-australia.com.au>

and:

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

7. operation of the CAPL RCA in an efficient and trustworthy manner and in accordance with the Accredited Documents and all relevant Approved CPs;
8. approval of 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. issuing of Certificates for Subordinate CAs in accordance with the certificate registration process described in this CP;
11. publication of issued Certificates in the CAPL X.500 Directory;
12. making of reasonable inquiries to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level in the CAPL PKI Hierarchy;
13. revocation of Certificates in accordance with the certificate revocation process described in this CP;
14. posting of details of revoked Certificates in a Certificate Revocation List ("CRL") in the CAPL X.500 Directory;

15. conduct of regular internal security audits;
16. facilitation of the conduct of regular audits by NOIE-authorized external auditors relating to the maintenance of Gatekeeper Accreditation status;
17. conduct of compliance audits of Subordinate CAs when Certificate renewal is due.

1.3.1.2.1 CAPL RCA Contact Details

The contact details for the CAPL RCA are:

Name:	Baltimore Certificates Australia Pty Limited
ACN:	075878867
Trading as:	CAPL
OID:	1,2,36,75878867,3
Postal Address:	Level 5, 1 James Place, North Sydney NSW 2060 Australia
Phone:	+61 2 9409 0300
Fax:	+61 2 9409 0301
Domain Name:	http://www.certificates-australia.com.au
E-mail Address:	info@certificates-australia.com.au
Contact:	General Manager – BCAPL

1.3.1.3 Subordinate Certification Authorities

Details of all Subordinate CAs can be found in the relevant CPs.

1.3.2 Registration authorities

The identity of the CAPL RCA is confirmed by the PAA using the procedures laid down in Section 3.1, *Initial registration* of this CP.

The identities of the CAPL RCA CAOs are confirmed by the PAA using the same procedures as are used for confirming the identity of the CAPL RCA.

The CAPL RCA is responsible for checking Evidence of Identity (“EOI”) and collecting Certificate information for and about Subordinate CAs only.

The CAPL RCA CAOs are the administrative interface to the RCA, and are used to submit registration, suspension and revocation requests pertaining to Subordinate CAs to the CAPL RCA.

1.3.3 Subscribers

The CAPL RCA does not issue Certificates to Subscribers, therefore it is not responsible for checking of EOI and collection of Certificate information for and about Subscribers.

1.3.4 Applicability

Certificates supported by this CP are limited to:

1. the self-signed CAPL RCA Certificate itself;
2. the associated CAO Certificate which acts as an administrative interface into the CAPL RCA;
3. Subordinate CA Certificates issued by the CAPL RCA.

1.3.4.1 Applicable Certificate usage

Certificates issued under this CP are used to verify the chain of trust for all Subordinate CAs within the CAPL PKI Hierarchy. The CAPL RCA Certificate contains the CAPL RCA's Public Key and information about its validity.

1.4 Contact Details

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

**General Manager
Baltimore 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

1.4.1 Specific administration organisation

This CP is administered by CAPL.

1.4.2 Contact person

See Section 1.4, *Contact Details*.

1.4.3 Person determining CPS suitability for this policy

See Section 1.4, *Contact Details*.

2. General Provisions

2.1 Obligations

This section covers the obligations of CAPL and the CAPL RCA to all entities relying on Certificates issued under the CAPL PKI Hierarchy.

2.1.0 CAPL Obligations

CAPL shall provide a secure certification infrastructure that enables the issue of Public Key Certificates. The CAPL RCA is the highest point of trust within the infrastructure.

2.1.0.1 CAPL PAA Obligations

The CAPL PAA has the right to alter or amend this CP, and to publish on the CAPL Websites the amended CP but any changes must be approved by the NOIE.

The CAPL PAA shall:

- specify the time from which the new or amended CP will apply;
- consult with and notify NOIE and customers who are receiving certification services from CAPL under this CP 30 days prior to effecting any change to this CP.

Nothing in this provision shall prevent the CEO, NOIE from revoking or suspending the Accreditation status of CAPL or this CP.

2.1.1 CAPL RCA Obligations

The CAPL RCA obligations are:

1. to comply with all Gatekeeper Accredited Documents, Policies, Criteria and procedures;
2. to comply with applicable law;
3. to maintain the CPS and this CP;
4. to comply with, and ensure that its employees comply with, the conditions and obligations set out in this CP and the practices set out in the approved CPS;
5. to publish its CAPL RCA Hash on the CAPL Websites;
6. to advise Subordinate CAs of their obligations under this CP and the CPS and make accessible a copy of this CP and the CPS to each Subordinate CA;
7. to issue Subordinate CA Certificates to Subordinate CAs;
8. to generate Subordinate CA Certificates only on receipt of properly formatted and verified Certificate requests;
9. to issue Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
10. to establish the CAPL X.500 Directory to hold information pertaining to the status of all Certificate holders under this CP;
11. to receive suspension and revocation requests and take appropriate action;
12. to make reasonable enquiries in accordance with the arrangements agreed with Subordinate CA 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. to promptly notify a Subordinate CA in the event that the CAPL RCA initiates revocation of their Certificates;
14. to issue a new Subordinate CA Certificate to a Subordinate CA whose Keys have been compromised, or are suspected to have been compromised, after receiving a properly formatted and verified request from the Subordinate CA for a new Subordinate CA Certificate;
15. to conduct compliance audits of Subordinate CAs when Certificate renewal is due;
16. to facilitate the conduct of regular audits by NOIE-authorized external auditors to maintain Gatekeeper Accreditation status.

2.1.2 RA obligations

Reserved.

2.1.3 Subscriber obligations

Reserved.

2.1.4 Relying party obligations

Relying Party obligations are set out in the CP under which the Certificate on which the Relying Party is relying was issued, and the Relying Party Agreement (if any).

2.1.5 Repository Obligations

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

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

Repository obligations are therefore incorporated into the relevant Subordinate CA CP.

2.2 Liability

2.2.0 CAPL liability

2.2.0.1 CAPL PAA liability

The members of the CAPL PAA shall not be held liable for any CP created, modified or used within the CAPL PKI Hierarchy.

2.2.0.2 CAPL RCA liability

The CAPL RCA certifies Subordinate CAs under the terms and conditions of this CP to issue Certificates that comply with the Gatekeeper schema.

The CAPL RCA is not liable for the operation of any Subordinate CA (except the CAPL OCA) or any consequence of malfeasance, tort or contractual breach arising from the operation thereof, except to the extent that the Subordinate CA was operating in accordance with the CP and CPS.

2.2.1 CA Liability

CA liability is set out in the relevant Subordinate CA's CP and Agreement(s). Such CPs are not to be inconsistent with the terms and conditions of this CP.

2.2.2 RA Liability

RA liability is set out in the relevant Subordinate CA's CP and Agreement(s). Such CPs are not to be inconsistent with the terms and conditions of this CP.

2.2.3 End Entity Liability

The liability régime applying to a Subscriber or a Relying Party is set out in the relevant CP and any applicable Subscriber/Relying Party Agreement(s).

2.2.4 Liability of the Commonwealth

Notwithstanding any other provisions of this CP:

1. the Commonwealth makes no representations, and offers no warranties or conditions, express or implied, in relation to:
 - the activities or performance of any of the entities participating in a PKI whose Root CA is the CAPL RCA (“PKI Entities”) which are carried out under, or in relation to, this CP; or
 - if relevant, the services or products of a particular PKI Entity; and
2. the PKI Entities acknowledge and agree that except to the extent that a Commonwealth agency is carrying out the role of a PKI Entity (in which case the liability of the Commonwealth will be determined in accordance with the provisions set out in this Section 2.2, *Liability*), the Commonwealth disclaims any and all liability of any kind whatsoever for any loss or damage caused to, or suffered by, any person, including a PKI Entity as a result of:
 - an entity described in this CP carrying out, or omitting to carry out, any activity described in, or contemplated by, the Accredited Documents;
 - the Commonwealth carrying out, or omitting to carry out, any activity related to the Gatekeeper accreditation process; or
 - a negligent act or omission of the Commonwealth.

2.3 Financial responsibility

2.3.1 Indemnification by relying parties

Reserved.

2.3.2 Fiduciary relationships

Issuing Certificates in accordance with this CP does not make CAPL or the CAPL RCA an agent, fiduciary, trustee, or other representative of any End Entity.

2.3.3 Administrative processes

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

2.3.4 Baltimore Certificates Australia Pty Limited

Baltimore Certificates Australia Pty Limited is a wholly owned subsidiary of Baltimore Technologies Pty Limited, a company incorporated in Australia. Baltimore Technologies Pty Limited is wholly owned by Data Innovation Benelux BV, a company incorporated in the Netherlands. Data Innovation Benelux BV is wholly owned by Baltimore Technologies plc, a publicly listed company on the London Stock Exchange.

2.3.5 Client managed CA and RA services

CAPL customers who manage Subordinate CA and RA services issuing Gatekeeper Certificates within the CAPL PKI Hierarchy must be Gatekeeper Accredited.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

This CP is governed by the laws in force in the Australian Capital Territory, Australia.

Furthermore, all parties using or relying upon this CP submit to the non-exclusive jurisdiction of the courts, including the Federal Court in the Australian Capital Territory and all Courts of Appeal.

2.4.1.1 Applicable contract structure

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

- **Gatekeeper CA Head Agreement:** Establishes a contractual relationship between CAPL and the Commonwealth of Australia, represented by NOIE, for the provision of CA Services under Gatekeeper.
- **RCA - CA Operating Agreement:** Describes contractual arrangements under which CAPL will enable a Subordinate CA to operate and includes the roles and responsibilities of each party. This document includes a copy of the CAPL Concept of Operations (“CONOPS”) document.

2.4.1.2 Subordinate contract structure

- **Product Licensing Agreement:** Describes the licence terms and conditions of products provided to CAPL customers which are used to deliver the CAPL CA Service Provider’s services.

2.4.2 Severability, survival, merger, notice, assignment

2.4.2.1 Severability

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

2.4.2.2 Survival (Continuing obligations)

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

2.4.2.3 Merger

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

2.4.2.4 Notice

Notice, consent, request or any other communication under this CP must be in one of the following forms unless the party to be notified is CAPL itself:

1. Electronically — provided that the notice has been digitally signed by a subordinate entity that is part of the CAPL PKI Hierarchy under an Approved CP;
2. In writing — provided that the notice:
 - is left at the recorded address in this CP, or the recorded address of the Certificate holder; or,
 - is sent by prepaid post (airmail if posted to or from a place outside Australia) to the recorded address in this CP, or the recorded address of the Certificate holder; or,
 - is sent by facsimile to the facsimile number recorded in this CP, or the facsimile number of the Certificate holder.

A notice, consent, request or any other communication is deemed to be received:

1. if sent electronically, at the time that the notice is received by the recipient's host machine, and only after:
 - the digital signature has been verified and authenticated; and
 - the CP has been verified as an Approved CP.

2. if delivered by hand, when it is actually delivered to the recipient;
3. if sent by letter, three days after posting (seven days, if posted to or from a place outside Australia);
4. if sent by facsimile, at the time of dispatch, provided the sender obtains a transmission report which confirms that the facsimile was successfully sent in its entirety to the facsimile number of the recipient.

2.4.2.4.1

Notice action

Notices under this CP will be issued by CAPL for the following events:

- establishment of a new Approved CP;
- change or alteration of an existing Approved CP;
- revocation of the CAPL RCA's or a Subordinate CA's Certificates;
- renewal of the CAPL RCA's or a Subordinate CA's Keys or Certificates.

Notices will also be issued, or publication made, by the relevant entity in the CAPL PKI Hierarchy for the following events:

- revocation of a Certificate;
- renewal of a Key or Certificate.

Parties requiring publication or receipt of notice under this CP are required to provide notice of:

- changes in their address including postal and email addresses;
- security compromises of their Private Key(s);
- changes in information which would change the basis upon which the Certificate has been issued; and,
- any other event pertinent to the maintenance of the provisions of this CP.

2.4.2.4.2

Notice acknowledgment

Specific acknowledgment is not required except as otherwise provided for under this CP.

2.4.2.5

Assignment and novation

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

1. to a Gatekeeper Accredited entity;
2. with the prior agreement of the other party; and
3. with the prior agreement of NOIE.

2.4.3 Dispute resolution procedures

The dispute resolution provisions are taken to cover any area addressed by this CP. This includes but is not limited to:

- differences in or between any Gatekeeper Accredited CP;
- contractual matters arising out of this CP;

- subject to this CP, privacy policy and practice impacted by or on this CP.

2.4.3.1 Hierarchy of Certificate policy

In the event that a dispute arises between parties under the CAPL PKI Hierarchy the following order of precedence will apply:

1. where the subject of the dispute is covered by a contract (e.g. between the CAPL RCA and a Subordinate CA) then the contract shall prevail;
2. where the subject of the dispute is covered wholly within this CP (e.g. between two Subordinate CAs) then this CP shall prevail.

2.4.3.2 Process

If a dispute arises in connection with this CP, the parties undertake in good faith to use all reasonable endeavours to settle the dispute by negotiation or mediation.

This process is not binding where the dispute is between two CAPL-owned entities.

If the parties are not able to resolve a dispute within a reasonable time from the date the dispute first arises, then the parties shall agree to jointly appoint an independent arbitrator, having appropriate qualifications and practical experience (“Arbitrator”), for the purpose of resolving the dispute and agree to be bound by the decision of that Arbitrator.

If the parties are not able to agree on an Arbitrator within 14 days from the date the parties agreed to appoint an Arbitrator, then the parties agree to appoint the person nominated by the President for the time being of the Australian Institute of Arbitrators. Either party may request the President of the Australian Institute of Arbitrators to make such a nomination.

The parties will promptly furnish to the Arbitrator (imposing appropriate obligations of confidentiality) all information reasonably requested by the Arbitrator relating to the dispute.

The Arbitrator will use all reasonable endeavours to render the Arbitrator’s decision within 30 days following receipt of the information requested or, if this is not possible, as soon as practical thereafter, and the parties must co-operate fully with the Arbitrator to achieve this objective.

The parties will share equally the fees and expenses of the Arbitrator except if the dispute involves an End Entity, in which case the expenses of the Arbitrator will be shared as agreed between the customer, CAPL and any other entity involved.

If a party does not think that the process described above is appropriate, the parties can agree a different process that is more suitable to the circumstances of the dispute.

2.5 Fees

2.5.1 Certificate issuance or renewal fees

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

2.5.2 Certificate access fees

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

2.5.3 Revocation or status information access fees

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

2.5.4 Fees for other services such as policy information

No fee is to be levied for access to this CP or the approved CPS via the Internet. A fee may be charged for printed copies of this CP or the CPS. Printed copies of this CP are available from CAPL for a fee of \$AUD5.00 plus postage and packaging.

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

2.5.5 Refund policy

A refund policy may apply to nominated fees. This may be done by publishing the refund policy on the CAPL Websites or directly to the OCA.

2.6 Publication and repository

2.6.1 Publication of RCA information

This CP is published under the International Standard Book Number (“ISBN”) system.

2.6.1.1 Electronic publication

This CP is published electronically in PDF format, and the hash of this document is published on the CAPL Websites.

2.6.1.2 Hard copy publication

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

<p>General Manager Baltimore Certificates Australia Pty Ltd Level 5, 1 James Place NORTH SYDNEY NSW AUSTRALIA</p>

2.6.2 Frequency of publication

Publication frequency is as follows:

1. New versions of this CP and the 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 CP or of the CPS on the CAPL Websites.

Access to Certificate information (including CRLs) within the CAPL 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 all Public Keys, Certificates and public user information is the CAPL X.500 Directory. The CAPL X.500 Directory may be accessed via the CAPL Websites.

2.6.4.1 X.500 Directory functions

The CAPL X.500 Directory is provided for the retention of information about:

1. Subordinate CAs and Registration Authorities operating under the CAPL RCA;
2. Subscribers who agree to the publication of their Certificate information.

The CAPL X.500 Directory serves as a repository for a list of:

1. active Certificates (new and renewed);
2. suspended Certificates (CRL);
3. revoked Certificates (CRL);
4. expired Certificates.

The CAPL X.500 Directory shall not publish:

1. detailed information on how or why a Certificate has been revoked;
2. any information pertaining to a Subordinate CA that is not contained in the Certificate, unless the CA agrees to publish such information.

2.6.4.2 X.500 Directory contact details

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

Name:	Baltimore Certificates Australia Pty Limited
ACN:	075878867
Postal Address:	Level 5, 1 James Place, North Sydney NSW 2060, Australia
Phone:	+61 2 9409 0300
Fax:	+61 2 9409 0301
Domain Name:	www.certificates-australia.com.au
E-mail Address:	info@certificates-australia.com.au
Contact:	General Manager – BCAPL

2.6.4.3 X.500 Directory availability

The CAPL X.500 Directory will normally be available 7 days a week, 24 hours a day.

2.6.4.4 Repository Publication

The CAPL X.500 Directory promptly publishes new Certificates and changes in Certificate status, including revocation, notices of suspension and expiry.

The CAPL X.500 Directory is published on the CAPL Websites.

2.6.4.5 CRL Publication

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

Refer to the CAPL CPS for more detailed information on this subject.

2.7 Compliance Audit

2.7.0 Gatekeeper Evaluation

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

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

2.7.1 Frequency of entity compliance audit

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

1. within one year of the commencement of CAPL RCA operations; and
2. at any time that is deemed warranted by NOIE, in order to maintain Gatekeeper accreditation; and
3. at any other time that it deems warranted and at its own expense, provided a minimum of one month's notice is given to the entity that is to be audited.

2.7.2 Identity/qualifications of auditor

Any firm or person contracted to perform an audit on the CAPL RCA or a Subordinate CA must have significant relevant experience in the application of PKI and cryptographic technologies.

Where the audit is for the purpose of maintaining Gatekeeper Accreditation, the auditor must also be approved by NOIE.

2.7.3 Auditor's relationship to audited party

Aside from the audit function, the auditor and audited party shall 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

Areas to be audited include:

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

2.7.5 Actions taken as a result of deficiency

Copies of the audit report must be submitted to:

- General Manager — Baltimore Certificates Australia Pty Limited;
- NOIE (In – Confidence);
- the audited body.

When irregularities are found, the General Manager — Baltimore Certificates Australia Pty Limited shall promptly oversee or implement appropriate corrective action.

2.7.6 Communication of results

Audit results are considered to be sensitive commercial information. Unless otherwise specified in a contract, they will be protected in accordance with Section 2.8, *Data protection and privacy*.

2.8 Data protection and privacy

2.8.1 Types of information to be protected

2.8.1.1 Personal information

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

The Act specifies eleven 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 it were an Agency of the Commonwealth.

2.8.1.2 Tax File Number legislation

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

2.8.1.3 Registration information

The CAPL RCA is registered by authorisation from the CAPL PAA. As no proof of identity information is required for CAPL to register its own RCA, the official letter of authorisation shall constitute all registration information.

2.8.2 Types of information that may be disclosed

2.8.2.1 Certificate information

As the CAPL PAA authorises the creation of the CAPL RCA, the only information noted on the official letter of authorisation is that information which will appear in the X.509 V3 Certificate.

Information embodied in the Certificate held as part of the registration record is not considered to be confidential. All other information concerning the registration record will be considered confidential. This provision does not operate to prevent publication of the Certificate information.

2.8.3 Disclosure of Certificate revocation/suspension information

If the CAPL RCA Certificate is suspended, the Certificate will continue to be active but the CRL will show that the Certificate is suspended. During the period of suspension no Relying Party should rely on transactions signed by Private Keys associated with Certificates issued by the CAPL RCA itself or any of its Subordinate CAs.

2.8.3.1 Disclosure of Certificate suspension information

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

2.8.3.2 Disclosure of Certificate revocation information

Certificate revocation information contained in a CRL which is publicly available via the CAPL X.500 Directory.

Where the CAPL RCA Certificate is revoked, all Subordinate CAs are notified and a notice is placed on the CAPL Websites.

Note that detailed information considered in making a decision to revoke a Certificate will not be disclosed by CAPL — only the fact of revocation and a standard reason code will be disclosed through the CAPL X.500 Directory.

2.8.4 Release to law enforcement officials

No document or record belonging to or held by any entity in the CAPL PKI Hierarchy will 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.

2.8.5 Release as part of civil discovery

No document or record belonging to or held by any entity in the CAPL PKI Hierarchy will 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 a registration record has full access to that record, and is empowered to authorise release of that record to another party. A person will not have access to any subject's registration record unless formal authorisation is given by the subject.

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 an Approved CP; or,
2. by application in writing.

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

2.8.7 Other information release circumstances

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

2.9 Intellectual Property Rights

2.9.1 General provision

CAPL warrants that it is in possession of, or holds licences for the use of, hardware and software in support of this CP.

CAPL further warrants that operational use of this CP does not infringe any Intellectual Property Rights of any third party.

The use of RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, IETF PKIX RFC2527, by S. Chokhani and W. Ford, March 1999, for drafting this CP is acknowledged.

2.9.1.1 Certificates

All Intellectual Property Rights including all copyright in all Certificates and all documents (electronic or otherwise) belongs to, and will remain the property of, CAPL.

CAPL grants to all End Entities the right to use any Certificate issued by any CA in the CAPL PKI Hierarchy for the purposes for which they were issued.

2.9.1.2 Distinguished names

Intellectual Property Rights in distinguished names shall vest in the CAPL RCA unless otherwise agreed in writing.

2.9.1.3 Gatekeeper

The use of the Commonwealth Government's Gatekeeper policy is acknowledged.

2.9.2 Copyright

2.9.2.1 General

The Intellectual Property Rights in this CP are the exclusive property of CAPL.

2.9.2.2 In OIDs

Copyright in the Object Identifiers ("OID") for the CAPL PKI Hierarchy vest solely in CAPL.

OIDs are not to be copied, used or otherwise dealt with in any way except as approved by the CAPL PAA.

3. Identification and Authentication

3.1 Initial registration

The application for the CAPL RCA is given in the form of a letter from the CAPL PAA to the General Manager — Baltimore Certificates Australia Pty Limited which outlines all the information required for the issue of the CAPL RCA Certificate.

3.1.1 Types of names

The CAPL RCA Distinguished Name complies with the X.520 Certificate standard.

Prior to 12th November 2000, the Distinguished Name for the CAPL RCA was:

Common Name:	Certificates Australia Root CA
Organisation:	Certificates Australia Pty Limited
Organisational Unit:	Not Applicable
Country:	AU

After this date, the Distinguished Name for the CAPL RCA is:

Common Name:	Certificates Australia Root CA
Organisation:	Baltimore Certificates Australia Pty Limited
Organisational Unit:	Not Applicable
Country:	AU

3.1.2 Need for names to be meaningful

Reserved.

3.1.3 Rules for interpreting various name forms

Reserved.

3.1.4 Uniqueness of names

Reserved.

3.1.5 Name claim dispute resolution procedure

Reserved.

3.1.6 Recognition, authentication and role of trademarks

Reserved.

3.1.7 Method to prove possession of Private Key

The CAPL RCA must satisfy itself that the Private Key in its possession does in fact correspond to the Public Key in its Certificate. This is done by signing and verifying a message.

3.1.8 Authentication of organisation identity

As the CAPL RCA Certificate is self-signed, Evidence Of Identity is not required.

3.1.9 Authentication of individual identity

Not applicable to this CP.

3.2 Routine Re-key

3.2.1 RCA Routine Re-key

CAPL RCA Keys and Certificates shall remain valid for a period of nine (9) years from the date of establishment.

Routine re-keying may be completed provided that:

1. the Certificates are valid (i.e. not expired) at the time the routine re-key falls due;
2. the CAPL RCA's identification details have not changed;
3. the CAPL RCA's Private Key has not been compromised.

3.3 Re-key after Revocation

After revocation of the CAPL RCA's Certificates, re-keying is by way of a new application prepared and approved by the CAPL PAA.

3.4 Revocation request

A request to revoke the CAPL RCA's Certificates is made in accordance with Section 4.4.3, *Procedure for revocation request*.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Application for a CAPL RCA Key and Certificate is by the unanimous resolution of the CAPL PAA.

4.2 Certificate Issuance

The CAPL RCA Key and Certificate are generated and issued promptly on receipt of an authorised application from the CAPL PAA.

The Certificate generation process, known as the “Certificate Signing Event”, requires, at a minimum, the following people to witness the event:

- one member of the CAPL PAA, and
- one independent witness.

All witnesses must complete a Certificate Witness Statement which certifies that they witnessed the Certificate generation and are satisfied that the Certificate meets the agreed structure defined in the Certificate Signing Event documentation.

4.2.1 Certificate issue process

As the CAPL RCA Certificate is a self-signed Certificate, a certificate request file is not needed. Using the software application, the Certificate information is entered into the software and the Keys and self-signed Certificate are generated using that information. The Private Key is then backed up for secure archival offsite and is security sealed and recorded in the Trusted Element register. On expiry of the CAPL RCA Certificate, the backup copy is destroyed but the Public Keys are archived for another 7 years from the date of expiry.

Detailed Backup and archiving procedures are defined in the CAPL System Security Plan.

4.3 Certificate acceptance

The CAPL RCA Certificate is deemed to have been accepted when the witnesses to the Certificate generation have signed their witness statements and certified that all information in the Certificate is correct.

4.4 Certificate suspension and revocation

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

On receipt by the CAPL PAA of a request to revoke the CAPL RCA Certificate, the CAPL PAA shall meet to verify the validity of the request. If it is valid, the CAPL PAA will instruct the CAPL RCA to suspend (but not revoke) the CAPL RCA Certificate forthwith. The CAPL PAA will then inform the NOIE of the suspension.

Subsequent to such suspension, the CAPL PAA shall consult with NOIE to decide the best course of action. Possible actions are revocation of the CAPL RCA Certificate or lifting of the suspension.

In the event that a revocation is required, the CAPL RCA shall inform all Subordinate CAs as soon as the decision has been made.

4.4.1 Circumstances for revocation

The CAPL RCA's Certificate is revoked in the event of:

1. the theft, loss, disclosure, modification, or other compromise or suspected compromise of the CAPL RCA's Private Key(s); or
2. the deliberate misuse by a trusted user of the CAPL RCA Keys and Certificates, or a substantial non-observance of operational requirements in a relevant agreement or associated CP or of the practices in the CPS; or
3. the cessation of operation of the CAPL RCA; or
4. the improper or faulty issue of a CAPL RCA Certificate; or
5. the material CAPL RCA Certificate information becoming inaccurate;
or
6. a properly formatted request being received from the CAPL PAA (for the CAPL RCA); or
7. a validated request being received from a third party authorised by law (for example, a Court of New South Wales).

4.4.2 Who can request revocation

Revocation of the CAPL RCA's Certificate can be initiated by:

1. the CAPL PAA; or
2. a third party authorised by law, for example a Court of New South Wales; or
3. the CEO, NOIE.

4.4.3 Procedure for revocation request

Revocation of the CAPL RCA's Certificate can only be initiated:

1. after consultation with NOIE; and
2. after the CAPL PAA has met and a resolution has been made to revoke the CAPL RCA's Certificate; and
3. a written authorisation to revoke the CAPL RCA's Certificate has been issued by the General Manager – Baltimore Certificates Australia Pty Limited to the CAPL Operations Manager.

Once the written authorisation is received, the CAPL RCA Certificate is revoked and:

1. the CAPL RCA Certificate is added to the CRL in the CAPL X.500 Directory; and
2. a notice is placed on the CAPL Websites; and
3. all Subordinate CAs are notified directly and immediately by the CAPL RCA.

4.4.4 Revocation request grace period

No grace period is allowed for revocation of the CAPL RCA. As soon as the CAPL PAA authorises such a revocation, it is actioned.

4.4.5 Circumstances for suspension

The CAPL RCA's Certificate is suspended by the CAPL RCA when:

1. there are reasonable grounds for believing that the CAPL RCA's Private Key has been compromised; or
2. there are reasonable grounds for believing that the media holding the CAPL RCA's Private Key is compromised; or
3. a properly formatted request is received in accordance with Section 4.4.7, *Procedures relating to suspension*.

4.4.6 Who can request suspension

Suspension of the CAPL RCA's Certificate may be initiated by:

1. the CAPL PAA;
2. NOIE;
3. a third party authorised by law, for example a Court of New South Wales.

4.4.7 Procedures relating to suspension

The procedure for suspension is available from the CAPL Websites.

The suspension notice on the CAPL RCA Certificate may only be removed:

1. after consultation with NOIE; and
2. after the CAPL PAA has met and a resolution has been made to lift the suspension of the CAPL RCA's Certificate; and
3. a written authorisation to lift the suspension of the CAPL RCA's Certificate has been issued by the General Manager – Baltimore Certificates Australia Pty Limited to the CAPL Operations Manager.

If the CAPL PAA decides not to lift the suspension of the CAPL RCA's Certificate, or the suspension cannot be lifted within the Suspension Period, revocation of the CAPL RCA's Certificate is initiated (see Section 4.4.3, *Procedure for revocation request*).

4.4.8 Limits on suspension period

Suspension shall be no longer than one business day ("Suspension Period").

4.4.9 CRL issuance frequency

At the time of revocation, the CRL in the CAPL X.500 Directory is updated.

4.4.10 CRL checking requirements

It is recommended that Relying Parties should check the validity and currency of a Certificate for every transaction.

4.4.11 On-Line revocation/status checking availability

CAPL provides an on line mechanism for downloading the CRL from the CAPL X.500 Directory to verify the status of Certificates issued under the CAPL PKI Hierarchy.

4.4.12 On Line revocation checking requirements

Under the CAPL PKI Hierarchy, it is recommended that the Relying Party check the CRL on a per transaction basis.

4.4.13 Other forms of revocation advertisements available

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

4.4.14 Checking requirements for other forms of revocation advertisements

Under the CAPL PKI Hierarchy it is recommended that the Relying Party check the CAPL Websites for any notices on a per transaction basis.

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 will maintain sufficient records and archives of information relating to the operation of the CAPL PKI Hierarchy to enable a proper audit to be conducted in accordance with the requirements of this CP, the CPS and any accrediting body.

4.5.1 Types of events 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;
5. audit records, including security related events;
6. formal correspondence, including emails;
7. revocation records, including CRLs.

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 maintained 'on site' for a minimum period of three months and a maximum period of twelve months.

The audit logs are retained in archives for a minimum period of nine years or such other time as required to meet the National Archives of Australia ("NAA") requirements, and then transferred to the NAA. If, on completion of that term, CAPL is required by a person to keep the audit logs on-line, CAPL may charge that person a fee for the provision of that service.

Detailed information on this subject can be found in the CPS.

4.5.4 Protection of audit log

Audit logs are signed using a Private Key specifically generated for this purpose (“Audit Log Private Key”). Audit log signatures can be verified using the Certificate associated with the Audit Log Private Key.

4.5.5 Audit log backup procedures

CAPL has established and maintains a detailed backup procedure for audit logs which is documented in the CAPL System Security Plan.

4.5.6 Audit collection system

The CAPL audit collection system is a combination of automated and manual processes performed by the operating system running the UniCERT software, the UniCERT software itself, and by operational personnel. The audit mechanisms and procedures used may be found in the CAPL System Security Plan.

Detailed information on audit collection may be found in the CPS.

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 PKI Hierarchy. This PSRR covers the overarching risks and threats that may impact the PKI.

Individual threat and risk assessment are required at each subordinate entity level.

4.6 Records Archival

4.6.1 Types of events recorded

The following information is archived by the CAPL RCA:

1. audit logs of the CAPL RCA;
2. Certificate request information;
3. Certificates generated;
4. complete back up registers;
5. formal correspondence relating to the CAPL RCA.

- 4.6.2 Retention period for archive
- 4.6.2.1 Secure maintenance of Keys
In accordance with OECD Guidelines for Cryptographic Policy only Public Keys are archived. They are archived in the form of the Certificates that contain them.
- 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 specifically required.

The 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 a longer period is specifically required.

The audit logs are archived securely on a CD ROM.
- 4.6.3 Protection of archive
Archive media are protected either by physical security, or a combination of physical security and cryptographic protection. Such media are also protected from environmental factors such as temperature, humidity, and magnetism.
- 4.6.4 Archive backup procedures
Archive backup procedures have been established to ensure complete restoration of current service or verification. Details are specified in the CAPL Disaster Recovery and Business Continuity Plan and the CAPL System Security Plan. These documents are not publicly available.
- 4.6.5 Requirements for time-stamping of records
Trusted third party time-stamping is not currently supported under this CP, but nothing in this CP will operate to prevent a third party from offering that service outside this CP.
- 4.6.6 Archive collection system
Archiving is performed by the CAPL operations staff delegated with the responsibility for doing so. Detailed procedures for backups, archiving and storage have been set out in the System Security Plan.

4.6.7 Procedures to obtain and verify archive information

The integrity of the archives is verified in accordance with the criteria set out in the System Security Plan:

1. annually at the time of the programmed security audit;
2. at any time when a full security audit is required;
3. at the time that the archive has been prepared.

4.7 Key changeover

CAPL RCA Key changeovers:

- require a minimum notice period of three months to all Subordinate CAs;
- must be formally applied for, using the application process outlined in Section 4.1, *Certificate Application*;
- must be effected in such a manner as to cause minimal disruption;
- must be manually effected — no automatic Key changeover processes are supported under the CAPL PKI Hierarchy.

4.8 Compromise and Disaster Recovery

The CAPL RCA maintains detailed documentation covering:

1. Contingency and Disaster Recovery Plan;
2. Configuration Baseline of the CAPL PKI Hierarchy;
3. OID hierarchies;
4. backup, archiving and offsite storage.

These plans will be made available to those persons responsible for conducting a security audit.

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

The Configuration Baseline Plan, Backup Plan, Archiving Plan, and Contingency and Disaster Recovery Plan shall provide data for identifying component failures, and subsequent service restoration.

4.8.2 Entity Public Key is revoked

The CAPL RCA and each Subordinate CA have established a Key and user compromise plan that addresses the actions to be taken in the event that the CAPL RCA Certificate is revoked. This is documented in the CAPL System Security Plan.

4.8.3 Entity Private Key is compromised

The CAPL RCA has established a Key and user compromise procedure that addresses the actions to be taken in the event that a Private Key is compromised. This procedure is documented in the CAPL System Security Plan.

The CAPL RCA shall promptly advise NOIE of any compromise or suspected compromise of its Private Keys.

4.8.4 Secure facility after a natural or other type of disaster

Backup, archive and offsite storage are managed in accordance with the Configuration Baseline of the CAPL RCA and its associated backup, archiving and offsite storage plans.

4.8.5 Contingency & Disaster Recovery Plan

Each element in the CAPL PKI Hierarchy is covered by a Contingency and Disaster Recovery Plan that addresses the actions to be taken in order to restore core business operations as quickly as practicable when system operations have been significantly and adversely impacted by fire, strikes, etc.

4.9 RCA 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 Hierarchy could occur, and to spell out the rights and obligations of the parties in these circumstances. The function of this section is also to ensure that:

1. the parties co-operate with each other in minimising any disruption that may be caused; and,
2. the parties' capacity to use the CAPL PKI Hierarchy 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 under which it will be necessary to activate the Business Continuity Plan are not set out in this CP. 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 be undertaken by:

1. the Commonwealth of Australia acting through NOIE; and
2. the Commonwealth agency receiving the certification products and/or services; and
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. above has ceased to provide products or services to the Commonwealth Agency for any reason including:

- the expiration of the contract; or
- the relevant contract is to be, or has been, terminated for default or for convenience; or
- 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.

Insofar as it is required, CAPL shall effect a transfer of Keys and Certificates to another Gatekeeper Accredited RCA (“Replacement RCA”) in a manner agreed with NOIE. For the purposes 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:

- CAPL will:
 - give to NOIE and any affected Commonwealth agencies 3 months’ prior written notice of its intention to terminate its CAPL RCA business operations; and
 - reasonably co-operate with NOIE and all relevant Commonwealth agencies in the selection of the Replacement RCA to take over the CAPL RCA business operations; and
 - transfer the Private Key of the CAPL RCA to the Replacement RCA, in a highly secure and trustworthy manner, which manner will be approved by NOIE; and
 - transfer the CRL and other directories of Certificates issued by the CAPL RCA to the Replacement RCA, in a highly secure and trustworthy manner, which manner will be approved by NOIE; and

- 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 is used to digitally sign the Subordinate CAs' Public Key Certificates is held by the Replacement RCA; and
 - provide a formal declaration concerning the destruction of the CAPL RCA Private Key (referred to above) to the CEO, NOIE, other relevant Commonwealth agencies and the relevant Subordinate CAs and RAs; and
 - 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 Subordinate CA Public Key Certificates for each Subordinate CA within the CAPL PKI Hierarchy that has been transferred;
- 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 would arise where, pursuant to a law (State or Commonwealth), it becomes 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 CEO, NOIE and the other members of the CAPL PKI Hierarchy in writing, or if writing is inappropriate the representative may advise by telephone, that the CAPL RCA will be immediately terminating its business operations.

In this case:

- all affected Commonwealth agencies and other members of the CAPL PKI 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 CAPL RCA, and the transfer of the CAPL RCA's Private Key to a Gatekeeper Accredited replacement RCA ("Replacement RCA");
- CAPL or its administrator/controller/liquidator or representative will:
 - 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 be approved by NOIE; and

- assist to the highest degree possible in the transfer of the CRL and other directories of Subordinate CA Certificates issued by the CAPL RCA to the Replacement RCA, in a highly secure and trustworthy manner, which manner will be approved by NOIE; and
- 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 is used to digitally sign Subordinate CA Public Key Certificates is held by the Replacement RCA;
- provide a formal declaration concerning the destruction of the CAPL RCA Private Key (referred to above) to the CEO, NOIE, relevant Commonwealth agencies and the relevant Subordinate CAs and RAs;
- 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 Subordinate CA within the CAPL PKI Hierarchy that has been transferred.

4.9.4 Subordinate CA Termination

The processes for termination of a Subordinate CA, both programmed and non-programmed, must be fully described in all CPs applicable to certificates that that Subordinate CA will issue.

4.9.5 Transfer of Root CA Data

The transfer of the Private Key of the CAPL RCA and the transfer of Subordinate CAs' Public Key Certificates to a Replacement RCA are dependent upon CAPL receiving a fair and just price for the transfer.

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 a secure office environment occupied by Baltimore Technologies Pty Limited.

The CAPL RCA is operated 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 CAPL RCA secure operating area is connected to a standard power supply. All critical components are connected to uninterruptible 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 CAPL 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 has a built-in 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 CAPL RCA secure operating area, to guard against the possibility of fire.

5.1.6 Media storage

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

5.1.7 Waste disposal

Paper documents and magnetic media containing the CAPL 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 a CAPL approved service.

5.1.8 Off-site backup

CAPL approved off site storage agents are used for the storage and retention of backup software and data. The backup procedures used are documented in the CAPL System Security Plan.

The off site storage:

1. has appropriate levels of physical security in place.
2. may be accessed by authorised personnel for the purposes of retrieving software and data between the hours of 9am and 4pm on Working Days in the state of New South Wales;

5.2 Procedural Controls

5.2.1 Trusted roles

In accordance with ACSI 33, responsibilities at CAPL RCA service workstations are shared by multiple roles and individuals to ensure that one person acting alone cannot circumvent the entire security of the system. 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 security policy described in CAPL's Information Systems Security Policy.

This is accomplished by creating separate roles and accounts on the CAPL RCA service workstations, each of which has a limited amount of capability. This method enables a system of “checks and balances” to operate between the various roles. The following roles have been established:

1. CA Operations Co-ordinators;
2. Facility Security Officer;
3. IT Security Manager.

The process for maintaining separation of roles is defined in the CAPL System Security Plan.

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. In particular:

1. the IT Security Manager always remains separate from the CA Operations Co-ordinators in order to provide an independent review of the audit log;
2. any task requiring the creation, backup or import into a database of a Private Key involves 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 undergo a formal vetting process conducted by the Australian Security Vetting Service.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The recruitment and selection practices for CAPL 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 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 CAPL RCA services personnel are trained in:

1. basic PKI concepts;
2. the use and operation of the CAPL RCA software;
3. documented CAPL RCA procedures;
4. computer security awareness and procedures;
5. how to explain to Subordinate 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 the CPS.

5.3.4 Retraining frequency and requirements

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

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

Remedial training is completed when recommended by audit comments.

5.3.5 Job rotation frequency and sequence

The CAPL RCA may implement formal job rotation practices. 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 CAPL RCA services personnel staff are submitted to appropriate authorities including, but not limited to, the IT Security Manager.

5.3.7 Contracting personnel requirements

CAPL 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

CAPL RCA services personnel shall have access to all relevant:

1. hardware and software documentation;
2. policy documents, including this CP;
3. operational practice and procedure documents, including the relevant CAPL approved CPS .

6. Technical Security Controls

6.1 Key Pair Generation

6.1.1 Key pair generation

CAPL RCA and CAPL RCA CAO Key pairs are generated and installed by the CAPL RCA using software that is listed on the EPL.

6.1.2 Private Key delivery to entity

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

6.1.3 Public Key delivery to certificate issuer

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

6.1.4 CA Public Key delivery to users

The self-generated CAPL RCA Public Keys will be published on the CAPL Websites.

6.1.5 Key sizes

The CAPL RCA Key length is 2048 bits.

6.1.6 Public Key parameters generation

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

6.1.7 Parameter quality checking

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

6.1.8 Hardware/software Key generation

CAPL RCA Key generation is performed software that is listed on the EPL.

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 are not used by the CAPL RCA.

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

CAPL RCA 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 CAPL RCA Private Key is stored in an encrypted file, 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

Cryptographic modules are not used by the CAPL RCA.

6.2.7 Method of activating Private Key

Private Keys are activated by the CAPL 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 CAPL RCA software application is terminated.

6.2.9 Method of destroying Private Key

The CAPL RCA software destroys Private Keys in memory when the software shuts down.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key archival

The CAPL RCA archives its Public Keys.

6.3.2 Usage periods for the Public Keys and Private Keys

The usage period for the CAPL RCA Private Keys and Public Keys is nine (9) 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 the certification authority software.

6.4.2 Activation data protection

No activation data other than access control mechanisms is required to operate the certification authority software.

6.4.3 Other aspects of activation data

No activation data other than access control mechanisms is required to operate the certification authority software.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

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

6.6 Life Cycle Technical Controls

6.6.1 System development controls

The software development controls applied in the development of the CAPL RCA software (UniCERT V3.1.2) have been evaluated under the Australasian Information Security Evaluation Programme (“AISEP”), and certified by the Australasian Information Security Evaluation Facility (“AISEF”) to meet the requirements of ITSEC E3.

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* and outlined in the CAPL System Security Plan.

6.6.3 Life cycle security ratings

The CAPL RCA has established a Protective Security Risk Review (“PSRR”) that identifies and addresses all high or significant life cycle security threats.

6.7 Network security controls

The CAPL RCA has established a PSRR that identifies and addresses all high or significant network security threats.

6.8 Cryptographic module engineering controls

Cryptographic modules are not used by the CAPL RCA.

7. Certificate and CRL Profiles

7.1 RCA Certificate Profile

7.1.1 Version number(s)

The CAPL RCA supports the use of X.509 Version 3 certificates, which contain v.3 in the version field.

7.1.2 Certificate extensions

The CAPL RCA supports the use of X.509 Version 3 certificate extensions and uses the following standard extensions within the CAPL RCA Certificate:

- NetscapeCertType (flagged non-critical);
- Certificate Policies (flagged non-critical);
- Basic Constraints (flagged critical).

7.1.3 Algorithm object identifiers

CAPL OIDs are not allocated to algorithms supported and used within the CAPL PKI Hierarchy. Only published Algorithm OIDs are used

The following hashing/digest algorithms are supported:

1. Secure Hash Algorithm-1
2. Message Digest 5 (“MD5”)

The following padding algorithms are supported:

1. ISO 9796
2. PKCS#1

The following encryption algorithms are supported:

1. RSA
2. DES

The following authentication algorithms are supported:

1. RSA
2. DSA

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

7.1.4 Name forms

Certificates used by the CAPL RCA contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields respectively.

7.1.5 Name constraints

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

7.1.6 Certificate policy Object Identifier

The OID of this CP is carried in the standard extension field of issued X.509 certificates and is published in Section 1.2.2, *CAPL RCA CP OID*.

7.1.7 Usage of Policy Constraints extension

The CAPL RCA supports the use of the Policy Constraints extension.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical certificate policy extension

See Section 7.1.2, *Certificate extensions*.

7.2 CRL Profile

7.2.1 Version number(s)

The CAPL RCA supports the use of X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

The CAPL RCA supports the use of X.509 Version 2 CRL entry extensions.

8. Specification Administration

CAPL operates a PAA which has the responsibility for setting certificate policy direction for the overall PKI. Contact details for the PAA are given in Section 1.3.0.2.1, *CAPL PAA Contact details*.

Normally subordinate to the PAA is a PMA, which is vested in the CAPL RCA or equivalent. In the case of this CP, the PAA and PMA are vested in the same authority, the PAA.

Each CP used under the CAPL PKI Hierarchy has been allocated an OID. The OID provides a unique identifier for each CP which includes a policy version number. Details of the OID for this CP may be found in Section 1.2.2, *CAPL RCA CP OID*.

8.1 Specification change procedures

8.1.1 Initial publication

The responsible authority for changes to this CP is the CAPL PAA. The CAPL RCA has received formal endorsement and been allocated an OID by the CAPL PAA.

The CAPL RCA is responsible for:

1. advising all subordinate entities of the CAPL RCA CP and its applicability;
2. forwarding a copy of the CAPL RCA CP to each Subordinate CA along with an advice about where the CP can be read;
3. advising each Subordinate CA of any changes made to this CP.

8.1.2 Change

Two forms of policy change are contemplated:

1. issue of a new CAPL RCA CP;
2. change or alteration of the existing CAPL RCA CP.

Where a change to the CAPL RCA CP is required, the OID of the policy will remain in force, however a new version number will be allocated by the PAA on endorsement of the CAPL RCA CP by the CAPL PAA.

Following approval, the CAPL PAA will facilitate publication of the new CAPL RCA CP.

Any changes to this CP must be made in accordance with the Gatekeeper CA Head Agreement.

8.2 Publication and notification policies

The new CAPL RCA CP is published on the CAPL Websites. Subordinate entities will be notified of changes to the CP as and when they occur.

All Subordinate CAs will be notified of any changes to this CP at least one week prior to its publication.

8.3 CP approval procedures

This CP must be endorsed by the CAPL PAA, certified by an Authorised Evaluator and approved by NOIE to maintain its Gatekeeper Accredited status.