



Baltimore Certificates On-Line

CAPL – P08 (BC – PU) - Business Continuity Policy
(Public)

Information in this document is subject to change without notice.

No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from Certificates Australia Pty Limited.

Written and published in Sydney, Australia, by Certificates Australia Pty Limited.

Copyright © 1999 Certificates Australia Proprietary Limited,
ACN 075 878 867.

All Rights Reserved.

Table of Contents

Introduction and Overview.....	1
Purpose	1
Scope of this document	1
Document structure.....	1
Amendment procedure.....	1
References.....	2
Management Process.....	3
Establishment	3
Responsibilities	3
Publication	3
Revision.....	4
Appendix A – Certificates Australia Pty Limited Business Continuity Policy (Public)	5
Introduction	5
Scope	5
Background	6
Service transition plan	7
CAPL obligations	8
CA Service obligations	8
End User certificates and keys.....	8
Successor CA CPS ₍₁₎	9
Nominated successor CA	9

IMPORTANT NOTE ABOUT THIS DOCUMENT

The information contained in this document is intended for personnel charged with the management and operation of the Certification Authorities owned and operated as Certificates Australia Pty Ltd, 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.

This document has been produced in accordance with the general provision of the Commonwealth's policy and guidelines on the protection of information and information technology environments.

Contact:

General Manager – Certificates On-Line
Certificates Australia Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
AUSTRALIA
Ph +61 29409 - 0300

The presence of the signature below indicates that personnel charged with operating the Certification Authority Services on behalf of Certificates Australia Pty Ltd will abide by the policies contained herein.

(BCOL Representative)

INTRODUCTION AND OVERVIEW

Purpose

This document gives guidance on how the Business Continuity Policy (Public) is prepared, managed and published. The Business Continuity Policy (Public) outlines a general strategy to be used by CAPL for the continuation of CA services to End Users in the event of the operational shutdown (“shutdown”) of:

- the CAPL RCA or Certificates Australia Pty Limited;
- any subordinate CA or RA within the CAPL hierarchy.

This document contains a copy of the Business Continuity Policy (Public) authorised for publication (attached as Appendix A). The Policy is consistent with CAPL’s ‘Business Continuity’ obligations under the “Head Agreement” with the Australian Commonwealth Government.

Scope of this document

This document:

1. defines the Business Continuity Policy (Public) for Certificates Australia Pty Limited (CAPL);
2. provides an overview on how the Policy is to be:
 - i.) prepared;
 - ii.) managed; and,
 - iii.) published.

Document structure

The document is divided into the following sections:

1. Introduction and Overview;
2. Management Process;
3. Appendix A - Certificates Australia Business Continuity Policy (Public).

Amendment procedure

As new standards emerge, or policy matters are identified for improvement, this document will be amended.

The responsibility for amending this document rests with the General Manager – BCOL naming convention for amendment notices shall be:

YY indicating the year the amendment was issued;

XXX where XXX represents a sequential number beginning with 000.

References

- Gatekeeper (Commonwealth Government)
- Gatekeeper compliant and GPKA accredited CP
- Gatekeeper compliant and GPKA accredited CPS

MANAGEMENT PROCESS

Establishment

Good management practice, Gatekeeper compliance and GPKA Accreditation criteria demand the production and commissioning of various policies and plans.

In accordance with these requirements, a Business Continuity Policy designated “Certificates Australia Pty Limited Business Continuity Policy (Public)” has been prepared and will be made public.

Note: Only policy documents carrying the designator “(Public)” shall be made public.

Responsibilities

The General Manager – Certificates On-Line is responsible for the:

- preparation, publication and communication of the Business Continuity Policy (Public);
- advising on matters relating to the Policy.

The CAPL Policy Approval Authority (PAA) is responsible for approving the publication of the Business Continuity Policy (Public).

All designated operational and support personnel are responsible for ensuring compliance with the Business Continuity Policy (Public).

Note: In the event of a conflict between a CAPL public policy document and a planning document, the planning document shall prevail.

Publication

This policy shall be published in accordance with the requirement for it to be made public. Unless otherwise stated by the General Manager – BCOL shall be published on the following websites:

www.certificates-australia.com.au

www.baltimore.com

Revision

The CAPL PAA shall review this document at regular intervals. At a minimum, it shall be reviewed annually.

APPENDIX A — CERTIFICATES AUSTRALIA PTY LIMITED BUSINESS CONTINUITY POLICY (PUBLIC)

Introduction

Good management practice, Gatekeeper compliance and GPKA Accreditation criteria demand the production and commissioning of various policies and plans.

In accordance with these requirements, Certificates Australia Pty Limited (CAPL) has prepared a Business Continuity Policy designated “Certificates Australia Pty Limited Business Continuity Policy (Public)”, published below.

The purpose of this Policy is to ensure that in the event of the operational shutdown (“shutdown”) of an element of the CAPL PKI hierarchy:

1. End User’s capacity to use Public Key Certificates is maintained; and,
2. the parties involved co-operate with each other in minimising any disruption that may be caused.

A copy of this document is published on the following websites:

www.certificates-australia.com.au

www.baltimore.com

Scope

This Policy covers the shutdown of:

1. Certificates Australia Pty Limited or the CAPL RCA;
2. the CAPL CA;
3. a Client CA within the CAPL PKI hierarchy;
4. the CAPL RA ;
5. a Client RA within the CAPL PKI hierarchy.

This Policy may be applicable to subordinate elements of the CAPL PKI hierarchy as described below.

Certificates Australia Pty Limited or CAPL RCA/ICA

In the event of a shutdown of Certificates Australia Pty Limited or the CAPL RCA/CA, the provisions of this Policy shall apply to all service elements within the CAPL PKI hierarchy.

CAPL CA

In the event of a shutdown of the CAPL CA, the provisions of this Policy shall apply to all Branded Client CAs and their subordinate RAs.

Client CA

In the event of a shutdown of a Client CA (whether a Branded Client CA or an Externally Operated Client CA), the provisions of this Policy shall apply to that client CA and its subordinate RAs.

CAPL RA

In the event of a shutdown of the CAPL RA, the provisions of this Policy shall apply to any Branded Client CAs that may register their users through the CAPL RA.

Client RA

In the event of a shutdown of a Client RA, the provisions of this Policy shall apply to that client RA.

Background

CAPL has signed a Head Agreement with the Australian Commonwealth Government for the provision of Certification Authority services. The Head Agreement mandates that a service provider must provide for a continuity of services in the event that CAPL ceases operations or a CA service within the CAPL PKI hierarchy shuts down.

A shutdown of CAPL or a CAPL PKI service element may be programmed or non programmed, as described below.

Programmed shutdown

A programmed shutdown is any event where:

1. the shutdown of a CA service has been predetermined; and,
2. the shutdown has been planned as a result of commercial decisions or corporate strategies; and,

3. the circumstances surrounding the shutdown allow a minimum of three month's notice to be given to subordinate elements.

Non programmed shutdown

A non programmed shutdown is any event where:

1. the shutdown of a CA service is unanticipated; and,
2. the shutdown occurs as a result of:
 - the exercising by CAPL, the GPKA or a client of provisions or prerogatives contained within a relevant contract or CP; or,
 - external circumstances; and,
3. the circumstances surrounding the shutdown allow less than three month's notice to be given to subordinate elements, including End Users.

Service transition plan

Where a CA service is to be transferred to a nominated successor CA service, a detailed Service Transition Plan (STP) shall be established by the CA service with the assistance, as appropriate of the GPKA and CAPL. The STP shall provide for the orderly transfer of records and services to the replacement CA service.

The STP shall conform with the CA termination requirements of a relevant Gatekeeper compliant and GPKA accredited CP and CPS.

An STP shall typically provide for:

1. timely notification to the GPKA, CAPL and End Users. In the case of a programmed shutdown, a minimum of three month's notice must be given;
2. the selection of a Gatekeeper compliant and GPKA Accredited CA service or PKI hierarchy to take over the business operations of the terminating CA service;
3. the transfer of the terminating CA service's keys and Certificates to the replacement CA service in a manner agreed with the Commonwealth Government and CAPL (or in the case of a terminating RA, the transfer of RA records in adherence to the privacy principles set in the Privacy Act);
4. the secure destruction of all private keys held by the terminating CA Service, that have been transferred to the replacement CA service;

CAPL obligations

In the event of the shutdown of a CA service within the CAPL PKI, CAPL shall as appropriate:

1. authorise or endorse the shutdown; and,
2. immediately notify the GPKA; and,
3. provide clients with as much notice as is reasonable and practical, in the event of a programmed shutdown this shall be a minimum of three month's prior notice; and,
4. provide clients with the options of:
 - shutting down CA services to their End Users; or
 - self-certifying their operations through the establishment of their own RCA; or
 - sourcing an alternative service provider; and,
5. to whatever extent is reasonable and practical, assist clients who choose to continue to provide CA services to their End Users including:
 - the progressive transfer of CA services and operational records to a nominated successor CA service;
 - the preservation of any records not transferred to a successor CA, service including in need a transfer of records to the National Archives of Australia, or another nominated party.

CA Service obligations

A terminating CA service shall:

1. establish an STP in terms of this document;
2. conform with the CA termination requirements of a relevant Gatekeeper compliant and GPKA accredited CP and CPS.

End User certificates and keys

In the event that a CA service shuts down:

1. all End User keys and certificates within the service's chain of trust may be revoked prior to the shutdown; or

2. all End User keys and certificates may be transferred to a replacement CA provided the certificates do not become operational within the chain of trust of the replacement CA service until after the shutdown of the terminating CA service; or
3. all End User certificates may be revoked prior to the shutdown of the terminating CA service and the End User keys may be transferred to the replacement CA service for the issue of new certificates, provided that such new certificates are not generated until after the shutdown of the terminating CA service.

Successor CA CP

The CP under which a nominated successor CA issues Certificates is a contractual matter between the client and the successor CA. In principle, however, to the extent that it is practical and reasonable:

1. the successor CA should assume the same rights, obligations and duties as the terminating CA;
2. the CPS₍₁₎ under which the successor CA issues Certificates should impose the same requirements and confer the same benefits as the CPS₍₁₎ under which the terminating CA issued Certificates;
3. the successor CA should agree to issue new Certificates to every End User whose Certificates were revoked due to the shutdown of the terminating CA, but only where the End User applies for a new Certificate and satisfies the CPS₍₁₎ initial registration and identification requirements.

Nominated successor CA

In the event that an externally operated client CA shuts down and the client chooses to continue to provide CA services to their end users, the nominated successor CA shall be the CAPL CA, unless otherwise specified in a relevant CP.