



Baltimore Certificates On-Line

CAPL - P05 (CK - MP).doc- Certificate Key
Management Plan (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 Baltimore Technologies Pty Limited.

Copyright © 1998, 2000 Baltimore Technologies Proprietary Limited,
ACN 003 823 461.

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
Responsibilities	3
Establishment.....	3
Publication.....	3
Revision	3
Appendix A — Certificates Australia Pty Limited Certificate Key Management Plan (Public).....	4
CA Private Key Security.....	4
Subscriber Key Recovery	4
Privileged User Management	5
Certificate Publication and Integrity.....	5
Key Generation and Transfer Mechanisms	5

IMPORTANT NOTE ABOUT THIS DOCUMENT

The information contained in this document is intended for Baltimore Technologies personnel charged with the management and operation of the Certification Authorities owned and operated as 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.

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 CA
Baltimore Technologies Pty Ltd
level 5, 1 James Place
NORTH SYDNEY NSW
AUSTRALIA

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

INTRODUCTION AND OVERVIEW

Purpose

The purpose of this document is to:

1. define the Certificate Key Management Plan (Public) for Certificates Australia Pty Limited (CAPL);
2. provide an overview on how the Plan is:
 - i.) produced; and
 - ii.) published.

This document contains a copy of the Certificate Key Management Plan (Public) authorised for publication (attached as Appendix A).

Scope of this document

This document gives guidance on how the Certificate Key Management Plan (Public) is prepared, managed and published. The Plan contains procedural statements that cover:

- CA private key security;
- subscriber key recovery;
- privileged user management;
- certificate publication and integrity;
- key generation and transfer mechanisms.

Document structure

The document is divided into the following sections:

1. Introduction and Overview;
2. Management Process;
3. Appendix A - Certificates Australia Pty Limited Certificate Key Management Plan (Public).

Amendment procedure

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

The responsibility for amending this document rests with the General Manager - CA. The 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)
- Recognised CAPL Gatekeeper compliant BALTIMORE
- Certificates Australia Pty Limited Security Policy (Public)

MANAGEMENT PROCESS

Responsibilities

The General Manager - BCOL is responsible for the:

- CAPL Certificate Key Management Plan (Public);
- preparation, publication and communication of the Certificate Key Management Plan (Public).

All designated operational and support personnel are responsible for ensuring compliance with the Certificate Key Management Plan (Public).

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

Establishment

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

In accordance with these requirements, a public planning document designated “Certificates Australia Pty Limited Certificate Key Management Plan (Public)” has been prepared and will be made public.

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

Publication

This Plan shall be published in accordance with the requirement for it to be made public. Unless otherwise stated by the General Manager - CA, it shall be published on the CAPL website at:

www.certificates-australia.com.au

Revision

The General Manager – CA shall review this policy at regular intervals. At a minimum, it shall be reviewed annually.

APPENDIX A — CERTIFICATES AUSTRALIA PTY LIMITED CERTIFICATE KEY MANAGEMENT PLAN (PUBLIC)

The Certificate Key Management Plan (Public) for Certificates Australia Pty Limited (CAPL) appears below. The CAPL Public Key Infrastructure (PKI) complies with this Plan.

The purpose of this Plan is to ensure that CAPL clients have the highest possible level of assurance that critical functions have been identified and provided at appropriate levels of trust.

A copy of this Plan is published on the Certificates Australia website at:

www.certificates-australia.com.au

CA Private Key Security

The Private Keys for CAPL operated CAs will be protected using the principle of “Defence In Depth” by which physical, administrative, logical and legal barriers operate together to provide layered protection to each CA Private Key.

The minimum physical security standard is set down in Australian Communications - electronic Security Instruction (ACSI) 33 CR2 standard.

The logical safeguards will be based on the standards required for a Highly Protected environment.

Subscriber Key Recovery

Where a CAPL Service Provider generates subscriber Key Pairs, the user’s private Confidentiality key will be automatically encrypted and archived. The archived key will be available for subscriber key recovery subject to the terms of any subscriber agreement that may be in place. A fee may be charged for recovery.

CAPL Service Providers will not archive:

- user public keys;
- user private Authenticity keys.

Privileged User Management

The efficient operation of CAPL Service Providers will require the establishment of the following privileged users:

1. System Supervisor;
2. System Administrator.

The System Supervisor will have root, administrator and user privileges.

The System Administrator will have administrator and user privileges.

Privileged users will be authorised to use their privileges where the use is consistent with:

1. duty statements;
2. normal course of duties;
3. exercise of delegated authority or responsibility.

The exercise of these privileges will not be permitted where:

1. the person exercising the privilege does so for personal gain;
2. the purpose may be malicious or cause harm to:
 - an individual;
 - the Service Provider system, or to its domains or services.

The creation of a privileged user account for a CAPL Service Provider will require the approval of the General Manager – BCOL.

Certificate Publication and Integrity

CAPL directory services will support the following Certificate states:

- Operational Use;
- Expiry;
- Revocation.

Certificate Owner access to master directories or to copies thereof will be limited to a name search enquiry that will allow the enquirer to determine within the span of the directory structure:

- the number of Certificates held by the nominated person;
- the type or grade of each Certificate;
- the status of each Certificate, i.e. valid, revoked or expired.

Key Generation and Transfer Mechanisms

Where a CAPL Service Provider generates subscriber Key Pairs, the key generation will be performed on a platform in a physically secure facility.

The Service Provider will ensure that the private keys and key transport passwords, e.g. Personal Identification Code (PIC) are not obtained by third parties prior to being received by the End User.

Private Keys and key transport passwords will be sent independently of each other using different methods of delivery, to mitigate against interception by a third party.