



Baltimore Certificates On-Line

CAPL – P04 (PP – PU) - Privacy 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, 1998 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
RESPONSIBILITIES.....	3
ESTABLISHMENT.....	3
PUBLICATION.....	3
REVISION.....	4
APPENDIX A – CERTIFICATES AUSTRALIA PTY LIMITED PRIVACY POLICY (PUBLIC)....	5
<i>Complain and Dispute Resolution Process.....</i>	<i>5</i>
<i>Review and Audit Process.....</i>	<i>6</i>
MANNER AND PURPOSE OF COLLECTION OF PERSONAL INFORMATION.....	6
<i>Pseudonymous certificates.....</i>	<i>6</i>
<i>Anonymous certificates.....</i>	<i>7</i>
SOLICITATION OF PERSONAL INFORMATION FROM AN END USER.....	7
COLLECTION OF PERSONAL INFORMATION GENERALLY.....	7
STORAGE AND SECURITY OF PERSONAL INFORMATION.....	7
<i>Use of Government Identifiers.....</i>	<i>8</i>
INFORMATION RELATING TO RECORDS KEPT BY RECORD-KEEPER.....	8
ACCESS TO RECORDS CONTAINING PERSONAL INFORMATION.....	8
ALTERATION OF RECORDS CONTAINING PERSONAL INFORMATION.....	9
RECORD-KEEPER TO CHECK ACCURACY ETC. OF PERSONAL INFORMATION BEFORE USE.....	9
PERSONAL INFORMATION TO BE USED FOR RELEVANT PURPOSES.....	9
LIMITS ON USE AND DISCLOSURE OF PERSONAL INFORMATION.....	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 Privacy Policy 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 02-9409-0300

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.

(ZAP Representative)

INTRODUCTION AND OVERVIEW

Purpose

The purpose of this document is to:

1. define the Privacy Policy (Public) for Certificates Australia Pty Limited (CAPL);
2. provide an overview on how the privacy policy is:
 - i.) prepared;
 - ii.) managed; and
 - iii.) published.

This document contains a copy of the Privacy Policy (Public) authorised for publication (attached as Appendix A).

Scope of this document

This document gives guidance on how the Privacy Policy (Public) is prepared, managed and published. The Privacy Policy (Public) contains Privacy Policy statements that cover the handling of personal information in the CAPL Public Key Infrastructure (PKI), in regard to information:

- collection;
- retention;
- use;
- disclosure;
- destruction.

Document structure

The document is divided into the following sections:

1. Introduction and Overview;
2. Management Process;
3. Appendix A - Certificates Australia Privacy Policy.

Amendment procedure

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

The responsibility for amending this document rests with the General Manager – Certificates On-Line. 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);
- Privacy Act 1988 - Section 14 Information Privacy Principles;
- Privacy Commissioner's National Principles for the Fair Handling of Personal Information;
- Recognised CAPL Gatekeeper compliant CPS₍₁₎.

MANAGEMENT PROCESS

Responsibilities

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

- CAPL Privacy Policy;
- preparation, publication and communication of the Privacy Policy (Public).

The CAPL Policy Approval Authority (PAA) is responsible for endorsing and approving the publication of the Privacy Policy (Public).

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

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

Establishment

Good management practice, Gatekeeper compliance and GPKA Accreditation criteria demand the production and commissioning of various policies and plans. There is also likely to be a legal requirement to comply with privacy principles as a result of State and Commonwealth Government Legislation to be passed in 1999.

In accordance with these requirements, a privacy policy designated “Certificates Australia Pty Limited Privacy Policy (Public)” has been prepared and will be made public on the Internet through a web page.

Note: Only policies carrying the designator “(Public)” shall be made public, with the exception of CPS₍₁₎.

Publication

This policy shall be published in accordance with the requirement for it to be made public. Unless otherwise stated by the General Manager – Certificates On-Line, it shall be published on the websites at:

www.certificates-australia.com.au

www.baltimore.com

Revision

The CAPL PAA shall review this policy at regular intervals. The minimum review period shall be annually.

APPENDIX A — CERTIFICATES AUSTRALIA PTY LIMITED PRIVACY POLICY (PUBLIC)

The Privacy Policy (Public) for Certificates Australia Pty Limited (CAPL) appears below. The CAPL Public Key Infrastructure (PKI) complies with this policy.

A copy of this policy is published on the websites at:

www.certificates-australia.com.au

www.baltimore.com

This privacy policy:

1. corresponds with Section 14 Information Privacy Principles (IPP) of the Privacy Act 1988, a copy of which may be located at the Australian Privacy Commissioner's web site:

www.privacy.gov.au

2. meets the requirements of the Australian Privacy Commissioner's National Principles for the Fair Handling of Personal Information (NPP), a copy of which may also be located at the above web site.

Note:

1. Where a higher test is identified by an IPP or an NPP then the higher test shall be applied in the CAPL PKI.
2. In the event that legislation is passed pertaining to privacy, CAPL shall amend this policy, and any associated planning document to meet the prescribed standards.

Complain and Dispute Resolution Process

Each community of interest within the CAPL PKI shall determine an appropriate complaint and dispute resolution process applicable to privacy issues. The process shall provide for right of appeal to an external industry or other suitable body, except where otherwise governed by law.

A complaint and dispute process has been included in each Certificate Policy Statement (CPS₍₁₎) applicable in the CAPL PKI hierarchy.

Review and Audit Process

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

This policy shall be externally audited by a qualified party no less than once every two years.

Manner and Purpose of Collection of Personal Information

The CAPL Public Key Infrastructure (PKI) shall collect such personal information as may be required for it to perform its designated functions. The collection of personal information shall be limited to:

- those elements of the CAPL PKI responsible for the registration of End Users;
- the requirements of a recognised CPS₍₁₎;
- lawful purposes;
- most information that is voluntarily and knowingly provided by the End User;

Information will only be acquired from third party organisations with the knowledge and consent of the End User

Pseudonymous certificates

The CAPL PKI supports the use of pseudonymous names provided that Certificate applicants are able to:

- meet the requirements of a prescribed Proof of Identity process in relation to their legal name; and,
- satisfactorily prove, using reasonable criteria, their right to the use of the requested pseudonymous name.

Pseudonymous names that may cause offence shall not be permitted.

Where an individual requests the use of a pseudonymous name, CAPL will keep their true identity confidential, subject to any legal requirements.

While the CAPL PKI supports the use of pseudonymous names, such use is subject to the determination of each community of interest. Particular communities may disallow the use of pseudonyms, or restrict their use to certain types or classes of certificates.

The CAPL PKI also supports the issue to an individual of multiple certificates in different names. Communities of interest may allow or disallow such multiple certificates at their discretion.

Anonymous certificates

The CAPL PKI is designed to support the use of certificates as a form of identification within a particular community of interest. An essential element in the CAPL PKI chain of trust is the binding of certificates to individuals who have met the requirements of a prescribed Proof of Identity process.

Anonymous certificates are not supported by the CAPL PKI.

Solicitation of Personal Information from an End User

Where information supporting the operational life cycle of a Certificate is requested from an End User the End User shall be informed:

- what information is being sought;
- why the information is required;
- what the information will be used for;
- to whom any of the information will be disclosed, including whether any of the information will be published.

Note that some information collected will be used in the End User's Public Key Certificate. The certificate will be posted on an X.500 Directory.

Collection of Personal Information Generally

Unless the collection of such information is a pre-requisite to the issuance of a Certificate for a particular community of interest, information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life shall not be collected, and then only with the informed consent of the End User concerned.

Storage and Security of Personal Information

All personal information collected shall be appropriately protected. Protection of such information shall include:

- physical protection of registration records;
- administrative guidelines that recognise and serve to protect the confidential nature of information collected;
- logical controls to prevent unauthorised or unintentional access or disclosure;
- a contractual hierarchy that ensures confidentiality of information.

The CAPL PKI archive its records for a period of seven years, unless otherwise specified.

Use of Government Identifiers

CAPL will require the production of a range of identification documents in order to establish the identity of Certification Authorities, Registration Authorities and End Users. These will include government identifiers such as passports, driving licences and notices of tax assessments. CAPL may record details of these identifiers but will hold them securely, not accessible to staff on a routine basis, and will not disclose them to any third parties other than as required under *Limits On Use and Disclosure of Personal Information* below. Except as prescribed by relevant legislation, the CAPL PKI shall not record individual's tax file numbers.

Information Relating to Records Kept by Record-Keeper

Personal information supporting the operational life cycle of a Certificate may be recorded by the CAPL PKI. Where such records are kept, the End User shall be entitled to receive, on written request, a general explanation of:

- CAPL's policy on the management of personal information;
- what personal information is held and for what purposes;
- how personal information is collected, held, used and disclosed including any publication of the information.

Access to Records Containing Personal Information

An End User has the right to request and view their own information held within the CAPL PKI. CAPL reserves the right to levy a reasonable fee for the production of such information.

An End user may also request confirmation that no information is held by the CAPL PKI other than:

- information published in their X.509 Certificate;
- Proof Of Identity information (registration records);
- billing information (as appropriate); or,
- information collected in the course of managing the certificate life cycle.

Recognised CPS₍₁₎ under the CAPL hierarchy shall have provisions that ensure the rights of the End User to gain access to their registration records.

Alteration of Records Containing Personal Information

If an End User can show that information held is not accurate, the relevant entity in the CAPL PKI shall amend the information to reflect the factual situation.

If the request for amendment cannot be supplied with evidence supporting the claim, CAPL reserves the right not to make the amendment, however a notice setting out the refusal to amend shall be given to the End User which sets out the grounds for refusal.

Record-Keeper to Check Accuracy Etc. of Personal Information Before Use

Each entity in the CAPL PKI shall take such steps as are reasonable given all the circumstances to verify the authenticity of information provided by an End User.

It should be noted that a recognised CPS₍₁₎ may set out criteria for acquiring and verifying information presented.

Personal Information To Be Used For Relevant Purposes

Information collected shall only be used by CAPL for the purpose of managing a certificate through its life cycle for the benefit of the End User and any relying parties.

A relevant purpose may also be stated in a recognised CPS₍₁₎.

Limits on Use and Disclosure of Personal Information

CAPL shall not use or disclose personal information for reasons outside the purpose of its collection except where:

- use or disclosure is required by law, for example disclosure to law enforcement agencies where a properly constituted warrant is produced;
- the End User specifically requests or approves of the use or disclosure.

Where such use or disclosure is required:

- a record shall be made and kept of the rationale for such use or disclosure;
- where appropriate the End User shall be notified of the use or disclosure.

Where CAPL discloses personal information to a contractor providing it with services, it will ensure that the contract requires the contractor to participate in a scheme of fair information handling.