



SECURITY DOMAIN

Baltimore Certificates On-Line

SDPL – 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 Security Domain Pty Limited.

Written and published in Sydney, Australia, by Security Domain Pty Limited.

Copyright © 1998 Security Domain Proprietary Limited,
ACN 082 074 575.

All Rights Reserved.

Table of Contents

SECURITY DOMAIN PTY LIMITED PRIVACY POLICY (PUBLIC)	2
MANNER AND PURPOSE OF COLLECTION OF PERSONAL INFORMATION	2
SOLICITATION OF PERSONAL INFORMATION FROM AN END USER	2
SOLICITATION OF PERSONAL INFORMATION GENERALLY	3
STORAGE AND SECURITY OF PERSONAL INFORMATION	3
INFORMATION RELATING TO RECORDS KEPT BY RECORD-KEEPER	3
ACCESS TO RECORDS CONTAINING PERSONAL INFORMATION	3
ALTERATION OF RECORDS CONTAINING PERSONAL INFORMATION	4
RECORD-KEEPER TO CHECK ACCURACY ETC. OF PERSONAL INFORMATION BEFORE USE	4
PERSONAL INFORMATION TO BE USED FOR RELEVANT PURPOSES	4
LIMITS ON USE AND DISCLOSURE OF PERSONAL INFORMATION.....	4

SECURITY DOMAIN PTY LIMITED PRIVACY POLICY (PUBLIC)

The Privacy Policy (Public) for Security Domain Pty Limited (SDPL) appears below. The SDPL Public Key Infrastructure (PKI) complies with this policy.

A copy of this policy is published on the Security Domain website at:

www.secdom.com.au

The Information Privacy Principles below correspond with Section 14 (Information Privacy Principles) of the Privacy Act 1988, a copy of which may be located at:

www.privacy.gov.au

Manner and Purpose of Collection of Personal Information

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

- those elements of the SDPL PKI responsible for the registration of End Users;
- the requirements of a recognised Certificate Policy Statement;
- lawful purposes;
- that information that is voluntarily and knowingly provided by the End User;

Information acquired from third party organisations shall require the advice and consent of the End User

Solicitation of Personal Information from an End User

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

- what information is being sought;
- why the information is required;
- what the information will be used for;
- whether the information will be published.

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

Solicitation 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.

Storage and Security of Personal Information

SDPL shall mandate that all 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 disclosure;
- A contractual hierarchy that ensures confidentiality of information.

The SDPL PKI shall comply with Commonwealth requirements for the archive and destruction of records held.

Information Relating to Records Kept by Record-Keeper

Information supporting the operational life cycle of a Certificate and its associated End User may be recorded by an operational element of the SDPL PKI. Where such records are kept, the End User shall be entitled to request:

- what information is being sought;
- why the information is required;
- what the information will be used for;
- whether the information will be published.

Access to Records Containing Personal Information

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

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

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

Recognised Certificate Policy Statements under the SDPL 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 SDPL PKI shall amend the information to reflect the factual situation.

If the request for amendment can not be supported, SDPL 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 SDPL 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 Certificate Policy Statement may set out criteria for acquiring and verifying information presented.

Personal Information to be Used for Relevant Purposes

Information collected shall only be used 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 Certificate Policy Statement.

Limits On Use and Disclosure of Personal Information

Information shall not be used or disclosed for reasons outside the purpose of its collection except where:

- use or disclosure is required by law;

- the End User specifically requests or approves of the disclosure;
- the use or disclosure is required in support of the Certificate life cycle.

Where such use or disclosure is required:

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