



**SECURITY DOMAIN**

## Baltimore Certificates On-Line

SDPL – P05 (CK – MP) - 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 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 Certificate Key Management Plan (Public) ..... 2

CA Private Key Security ..... 2

Subscriber Key Recovery ..... 2

Privileged User Management ..... 3

Certificate Publication and Integrity ..... 3

Key Generation and Transfer Mechanisms ..... 3

---

## **SECURITY DOMAIN PTY LIMITED CERTIFICATE KEY MANAGEMENT PLAN (PUBLIC)**

The Certificate Key Management Plan (Public) for Security Domain Pty Limited (SDPL) appears below. The SDPL Public Key Infrastructure (PKI) complies with this Plan.

The purpose of this Plan is to ensure that SDPL 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 Security Domain website at:

[www.secdom.com.au](http://www.secdom.com.au)

### **CA Private Key Security**

The Private Keys for SDPL 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 the 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 an SDPL 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.

SDPL Service Providers will not archive:

- user public keys;
- user private Authenticity keys.

## Privileged User Management

The efficient operation of SDPL 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 SDPL Service Provider will require the approval of the General Manager - Certificates On-Line.

## Certificate Publication and Integrity

SDPL 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 single 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 an SDPL 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.