



SECURITY DOMAIN

Baltimore Certificates On-Line

SDPL P03 (SP – PU) - Security 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 SECURITY POLICY (PUBLIC) 1

INTRODUCTION 1

PHYSICAL ENVIRONMENT..... 2

STANDARDS 2

OPERATIONS 2

TECHNOLOGY 3

PERSONNEL 3

LEGAL..... 3

AUDIT..... 3

SECURITY DOMAIN PTY LIMITED SECURITY POLICY (PUBLIC)

The Security Policy (Public) for Security Domain Pty Limited (SDPL) appears below, and is published on the Security Domain website at:

www.secdom.com.au

Introduction

Security Domain Pty Limited (SDPL) has established a Root Certification Authority (RCA) and corresponding PKI, within which it operates a number of Certification Authority (CA) services.

A fundamental concept underpinning the operation of a PKI is trust. Trust must be realised in each and every aspect of the service operation. Trust is viewed and defined by the impact of each of the following elements on the whole PKI:

- Physical environment;
- Standards;
- Operations;
- Technology;
- Personnel;
- Legal;
- Audit.

This document contains security policy statements describing the high level security requirements of the SDPL PKI for each of these areas. The SDPL PKI will operate in accordance with recognised international PKI standards.

Security Philosophy

The overarching security philosophy for all CA services is "Prevention, Detection and Considered Response". For the purpose of this policy, 'Considered response' means such actions as are justified having considered all the circumstances.

This philosophy means that the first aim of a CA service is to:

1. prevent any unauthorised action taking place;
2. detect and record any unauthorised action that has taken place;
3. take such action as may be required given the information available.

Protection of the SDPL PKI shall be rigorous in application, the "Defence In Depth" principle will be the prime security criteria for service operation in ensuring that physical, administrative, logical and legal barriers operate together to protect SDPL assets.

Physical environment

CA services are maintained in physically secure environments.

Standards

The security of the overall system is based on:

1. Australian Communication – electronic Security Instruction (ACSI) 33 – "Security in electronic Information Processing Systems";
2. Australian Communication – electronic Security Instruction (ACSI) 37 – "Australian Government Standards for the Protection of Information Technology Systems Processing Non-National Security Information at the Highly Protected Classification";
3. Supplement to Australian Communication – electronic Security Instruction ACSI 37 - "Certification Test Procedures for Information Systems Processing Highly Protected Data";
4. Information Technology Security Evaluation Criteria (ITSEC) E3;
5. Commonwealth Government's Protective Security Manual;

Operations

SDPL has established a PKI that meets the broad strategic direction of the existing international standards for the establishment and operation of a PKI.

Subordinate entities to the Root Certification Authority shall:

- conform to all SDPL PKI requirements;
- meet SDPL Policy Approval Authority requirements.

All private keys generated under the SDPL PKI shall be kept secret by their possessors and owners.

Key and certificate transport mechanisms shall ensure that only:

- lawful owners receive private keys and their associated certificates;
- authorised users receive public keys.

An X.500 directory is provided and maintained to facilitate access to:

- certificate status;
- public keys.

Planning documentation shall be prepared and maintained to ensure the correct operation of the service. The minimum documentation set includes:

- Concept of Operations
- Protective Security Risk Review
- System Security Plan
- Contingency & Disaster Recovery Plan

Technology

The RCA, CAs and RAs within the SDPL PKI shall achieve Certification of underlying technology elements to the ITSEC E3 level, in accordance with Section 23 of ASCI 33 - Multi Level Networks - Non-National Security Classified Systems.

Personnel

All personnel charged with the operation and management of the SDPL PKI shall be vetted to ensure their trustworthiness and suitability.

Legal

The contractual obligations, rights, and duties of each party in the PKI shall be identified in contract and reflected in Certificate Policy Statements, to ensure that the operation of the SDPL PKI is supported by a consistent legal infrastructure.

Audit

All CA services log security related or pertinent events. These logs are reviewed regularly to identify any attempted or actual security breaches, including misuse of access privileges.