

SECURITY DOMAIN

Baltimore Certificates On-Line

Certificate Practice Statement CPS₍₂₎
SDPL – L04 (CPS2) - SDPL PKI Certificates

Serial Number	
Release	Version 1.0
Status	Released
Issue Date	19-Mar-99

Copyright © 1999 Security Domain Proprietary Limited,
ACN 82074575

All Rights Reserved

No part of the contents of this document may be reproduced or distributed in any form or by any means without the prior written permission of Security Domain Proprietary Limited.

Security Domain Pty Limited
5th Floor, 1 James Place, North Sydney NSW 2060 Australia
Tel: +61 (0) 2 9409 0300 Fax: +61 (0) 2 9409 0301
www.secdom.com.au

Table of Contents

Table of Contents	1
CERTIFICATE PRACTICE STATEMENT	1
1. INTRODUCTION.....	2
1.1 Overview	2
1.1.1 Standards.....	3
1.1.2 Certificate types issued.....	3
1.1.3 Definitions	6
1.1.4 X500 Object Identifier hierarchy.....	6
1.1.5 Certificate Management Life Cycle	7
1.1.6 PKI Operational Infrastructure	12
1.1.7 Scope.....	15
1.1.8 Security Philosophy.....	15
1.1.9 Staffing Arrangements	16
1.1.10 Rights of Investigation	16
1.2 Identification	17
1.3 Community and Applicability	17
1.3.0 Policy Authorities.....	19
1.3.1 Certification Authorities	19
1.3.2 Registration Authorities.....	23
1.3.3 End Entities.....	24
1.3.4 Applicability	25
1.4 Contact Details	28
1.4.1 Specification administration organization.....	28
1.4.2 Contact person.....	28
1.4.3 Specification administration organization.....	28
1.4.4 Contact person.....	28
1.4.5 Person determining CPS suitability for this policy.....	29
2. GENERAL PROVISIONS	30
2.1 Obligations	30
2.1.0 SDPL Obligations.....	30
2.1.1 CA Obligations	31
2.1.2 RA Obligations	32
2.1.3 Subscriber Obligations.....	33
2.1.4 Relying party obligations	34
2.1.5 Repository Obligations	34
2.2 Liability.....	34
2.2.0 SDPL Liability.....	35
2.2.1 CA Liability	36
2.2.2 RA Liability	36
2.2.3 End Entity Liability	36

2.3	Financial responsibility	36
2.3.1	Indemnification by relying parties.....	36
2.3.2	Fiduciary relationships	36
2.3.3	Administrative processes.....	36
2.3.4	Security Domain Pty Limited.....	36
2.3.5	Client managed CA and RA services	37
2.4	Interpretation and Enforcement.....	37
2.4.1	Governing Law.....	37
2.4.2	Serverability, survival, merger, notice	37
2.4.3	Dispute resolution procedures	38
2.5	Fees	39
2.5.1	Certificate issuance or renewal fees.....	39
2.5.2	Certificate access fees.....	39
2.5.3	Revocation or status information access fees	39
2.5.4	Fees for other services such as policy information.....	39
2.5.5	Refund policy	40
2.6	Publication and repository	40
2.6.1	Publication of CA information	40
2.6.2	Frequency of publication.....	41
2.6.3	Access controls.....	41
2.6.4	Repositories	41
2.7	Compliance Audit.....	43
2.7.1	Frequency of entity compliance audit	43
2.7.2	Identity/qualifications of auditor.....	44
2.7.3	Auditor's relationship to audited party.....	44
2.7.4	Topics covered by audit.....	44
2.7.5	Actions taken as a result of deficiency.....	45
2.7.6	Communication of results	45
2.8	Confidentiality	45
2.8.1	Types of information to be kept confidential	45
2.8.2	Types of information not considered confidential	46
2.8.3	Disclosure of Certificate revocation/suspension information	47
2.8.4	Release to law enforcement officials	47
2.8.5	Release as part of civil discovery.....	47
2.8.6	Disclosure upon owner's request.....	47
2.8.7	Other information release circumstances	48
2.9	Intellectual Property rights.....	48
2.9.1	General provision.....	48
2.9.2	Copyright.....	49
3.	IDENTIFICATION AND AUTHENTICATION	50
3.0	General.....	50
3.0.1	CA and RA initial registration	50
3.0.2	End user initial registration.....	52
3.1	Initial registration	55
3.1.1	Types of names	55
3.1.2	Need for names to be meaningful.....	55
3.1.3	Rules for interpreting various name forms.....	56
3.1.4	Uniqueness of names	56

3.1.5	Name claim dispute resolution procedure	56
3.1.6	Recognition, authentication and role of trademarks	56
3.1.7	Method to prove possession of private key.....	56
3.1.8	Authentication of organization identity	57
3.1.9	Authentication of individual identity	57
3.2	Routine Rekey	57
3.3	Rekey after Revocation	58
3.4	Revocation request	58
4.	OPERATIONAL REQUIREMENTS	59
4.1	Certificate Application.....	59
4.2	Certificate issuance	59
4.2.1	Certificate issue process.....	59
4.3	Certificate Acceptance	61
4.4	Certificate Suspension and Revocation	62
4.4.1	Circumstances for revocation	62
4.4.2	Who can request revocation	63
4.4.3	Procedure for revocation request	64
4.4.4	Revocation request grace period.....	66
4.4.5	Circumstances for suspension	66
4.4.6	Who can request suspension	66
4.4.7	Procedure for suspension request.....	66
4.4.8	Limits on suspension period	66
4.4.9	CRL issuance frequency.....	67
4.4.10	CRL checking requirements.....	67
4.4.11	On-Line revocation/status checking availability.....	67
4.4.12	On Line revocation checking requirements.....	67
4.4.13	Other forms of revocation advertisements available.....	67
4.4.14	Checking requirements for other forms of revocation advertisements	67
4.4.15	Special requirements re key compromise.....	67
4.5	Security Audit procedures	67
4.5.1	Types of event recorded	67
4.5.2	Frequency of processing log.....	68
4.5.3	Retention period for audit log.....	68
4.5.4	Protection of audit log	68
4.5.5	Audit log backup procedures	68
4.5.6	Audit collection system	68
4.5.7	Notification to event-causing subject	69
4.5.8	Vulnerability assessments	69
4.6	Records Archival	69
4.6.1	Types of event recorded.....	69
4.6.2	Retention period for archive.....	70
4.6.3	Protection of archive	70
4.6.4	Archive backup procedures	70
4.6.5	Requirements for time-stamping of records	70
4.6.6	Archive collection system.....	70
4.6.7	Procedures to obtain and verify archive information.....	70
4.7	Key changeover.....	71

4.8	Compromise and Disaster Recovery	71
4.8.1	Computing resources, software, and/or data are corrupted	72
4.8.2	Entity public key is revoked.....	72
4.8.3	Entity key is compromised	72
4.8.4	Secure facility after a natural or other type of disaster.....	72
4.8.5	Contingency & Disaster Recovery Plan	72
4.9	CA Termination	73
4.9.1	Notice.....	74
4.9.2	End User keys and certificates	74
4.9.3	Successor CA CPS ₍₁₎	74
5.	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS .	76
5.1	Physical Controls.....	76
5.1.1	Site location and construction	76
5.1.2	Physical access	76
5.1.3	Power and air conditioning.....	76
5.1.4	Water exposures	77
5.1.5	Fire prevention and protection	77
5.1.6	Media storage	77
5.1.7	Waste disposal	77
5.1.8	Off-site backup.....	77
5.2	Procedural Controls.....	78
5.2.1	Trusted roles.....	78
5.2.2	Number of persons required per task	78
5.2.3	Identification and authentication for each role	78
5.3	Personnel Controls.....	78
5.3.1	Background, qualifications, experience, and clearance requirements	78
5.3.2	Background check procedures	79
5.3.3	Training requirements.....	79
5.3.4	Retraining frequency and requirements.....	79
5.3.5	Job rotation frequency and sequence.....	79
5.3.6	Sanctions for unauthorized actions.....	79
5.3.7	Contracting personnel requirements.....	80
5.3.8	Documentation supplied to personnel	80
6.	TECHNICAL SECURITY CONTROLS	81
6.1	Key Pair Generation and Installation	81
6.1.1	Key pair generation.....	81
6.1.2	Private key delivery to entity.....	81
6.1.3	Public key delivery to certificate issuer	81
6.1.4	CA public key delivery to users	81
6.1.5	Key sizes.....	81
6.1.6	Public key parameters generation	81
6.1.7	Parameter quality checking.....	82
6.1.8	Hardware/software key generation	82
6.1.9	Key usage purposes	82
6.2	Private Key Protection	82
6.2.1	Standards for cryptographic module.....	82
6.2.2	Private key (n out of m) multi-person control.....	82
6.2.3	Private key escrow.....	82

6.2.4	Private key backup.....	82
6.2.5	Private key archival.....	82
6.2.6	Private key entry into cryptographic module	82
6.2.7	Method of activating private key	83
6.2.8	Method of deactivating private key	83
6.2.9	Method of destroying private key.....	83
6.3	Other Aspects of Key Pair Management.....	83
6.3.1	Public key archival	83
6.3.2	Usage periods for the public and private keys.....	83
6.4	Activation Data	83
6.4.1	Activation data generation and installation	83
6.4.2	Activation data protection.....	83
6.4.3	Other aspects of activation data	84
6.5	Computer Security Controls	84
6.5.1	Specific computer security technical requirements.....	84
6.5.2	Computer security rating.....	84
6.6	Life Cycle Technical Controls.....	84
6.6.1	System development controls.....	84
6.6.2	Security management controls	84
6.6.3	Life cycle security ratings.....	84
6.7	Network Security Controls.....	84
6.8	Cryptographic Module Engineering Controls.....	84
7.	CERTIFICATE AND CRL PROFILES.....	85
7.1	Certificate Profile	85
7.1.1	Version number(s)	85
7.1.2	Certificate extensions	85
7.1.3	Algorithm object identifiers.....	85
7.1.4	Name forms	85
7.1.5	Name constraints.....	85
7.1.6	Certificate policy Object Identifier	86
7.1.7	Usage of Policy Constraints extension	86
7.1.8	Policy qualifiers syntax and semantics	86
7.1.9	Processing semantics for the critical certificate policy extension	86
7.2	CRL Profile.....	86
7.2.1	Version number(s)	86
7.2.2	CRL and CRL entry extensions	86
8.	SPECIFICATION ADMINISTRATION.....	87
8.1	Specification change procedures	87
8.1.1	Change	87
8.2	Publication and notification policies.....	88
8.3	CPS approval procedures	88
9.	Appendix A - Glossary.....	89
5.	Appendix B – CPS₍₁₎ Supported under this CPS₍₂₎	104

CERTIFICATE PRACTICE STATEMENT

SECURITY DOMAIN PTY LIMITED

CERTIFICATE PRACTICE STATEMENT

ACCREDITATION	SDPL
TYPE:	Standard Certificates
GRADE:	All Grades
VERSION No:	Version 0.4
STATUS:	Draft
ISBN No:	<To be issued>

1. INTRODUCTION

1.1 Overview

This Certificate Practice Statement CPS₍₂₎ is written to support the use of all grades of Standard Certificates (“Certificates”) under the Security Domain Pty Limited (SDPL) Public Key Infrastructure (PKI). The SDPL PKI is designed and is operated to comply with the broad strategic direction of the existing international standards for the establishment and operation of a PKI.

The SDPL PKI supports the creation and use of key pairs and of public key Certificates. Key pairs and public key Certificates are used in the provision of SDPL’s PKI Certificate services, including but not limited to:

1. authentication services (authentication, integrity and non-repudiation); and,
2. confidentiality services.

This CPS₍₂₎ provides factual information that describes the:

1. practices employed within the SDPL PKI to support Certificate services;
2. attendant use of technologies and processes to support the underlying operational infrastructure.

The practices described in this CPS₍₂₎ together with the technologies and processes referred to in other documents, illustrate the trustworthiness and integrity of SDPL’s Certificate operations from Certificate generation and signing to expiry.

SDPL PKI Certificate services

SDPL’s Certificate services provide a range of security and assurance levels to support the use of various Certificates created under the SDPL PKI. End User Certificates issued under the SDPL Root CA are used to conduct business with, or to engage in electronic transactions with other SDPL certificate holders.

The Certificates and associated CPS₍₁₎ supported under this CPS₍₂₎ range from contractual or signatory functions, through to high value financial arrangements such as purchase orders.

Certificates and associated supporting CPS₍₁₎ are also supportive of the use of either:

1. National privacy marking; or
2. National Security Classification markings.

Certificate services are to be considered as one of many elements in an overlapping framework of mechanisms, controls and procedures that protect and facilitate an organisation’s electronic business. It is critical that End Users and any other party relying upon a transaction supported by a Certificate:

1. understand the risks and threats of doing so; and,
2. ensure that appropriate mitigation and prevention measures have been put in place; and,
3. suitably position SDPL's Certificate services within an overall risk management plan.

Revisions

This CPS₍₂₎ undergoes a regular review process as prescribed by the SDPL Policy Approval Authority (PAA). Revisions of this document are identified through a configuration baseline schema and numbering convention.

1.1.1 Standards

This CPS₍₂₎ is referred to as the "Security Domain CPS₍₂₎".

The structure of this CPS₍₂₎ is based on the IETF PKIX 4 Draft, for more information see Section 1.1.1 *Standards* in a relevant CPS₍₁₎.

This CPS₍₂₎ differs from the PKIX 4 Draft standard only to the degree necessary to adequately describe the operational practices used within the SDPL PKI.

1.1.2 Certificate types issued

This CPS₍₂₎ supports the operation of:

1. all grades, types or classes of SDPL End User Certificates nominated in respective CPS₍₁₎;
2. nominated CA Certificates issued by the SDPL RCA;
3. nominated RA Certificates issued by SDPL CAs;
4. such other types of Certificates and supporting CPS₍₁₎ as may be approved by the SDPL PAA.

CPS₍₁₎ supported by this CPS₍₂₎ are listed in Appendix B – *CPS₍₁₎ Supported under this CPS₍₂₎* and are published on the web sites at:

www.secdom.com.au

www.baltimore.com

1.1.0.1 X.509 Certificate extensions

SDPL complies with the X.509 Version 3 standard. Part of this standard defines Certificate extensions that may be used to restrict the use of or convey additional information about a Certificate.

Certificate extensions consist of three fields:

1. type this field indicates the type of data in the value field;
2. criticality this indicates the importance of the information contained in the value field;
3. value this field contains the additional Certificate information.

The SDPL PKI supports Certificate extensions to provide additional information about a Certificate, as prescribed within a relevant CPS₍₁₎.

1.1.0.2 Policy qualifier extension

SDPL PKI certificates use Policy Qualifier extensions. Policy Qualifiers operate to convey important information for the attention of the Certificate owner or a relying party, including information such as:

1. liability; or,
2. information about the signing authority.

1.1.0.3 Approved Policy Qualifiers

The following Policy Qualifiers have been approved for use in SDPL PKI Certificates.

SDPL RCA Policy Qualifier

Security Domain Pty Limited Root CA Policy: Certificates issued under this policy are self signed and are issued by the Root CA itself.

User CA Policy Qualifier

Security Domain Pty Limited User CA policy: Certificates are issued under this policy to subordinate CAs established, and operated by, Security Domain Pty Limited.

Protocol key Policy qualifier

Security Domain Pty Limited Protocol Key Policy: Certificates issued under this policy are only to be used for communication between Security Domain Pty Limited and Registration Authorities.

Archive Authority Policy Qualifier

Security Domain Pty Limited Archive Authority Policy: Certificates are issued under this policy to Archive Authorities known to, or established by, Security Domain Pty Limited. Security Domain Pty Limited accepts no liability for the actions of these Archive Authorities.

Outsourced User CA Policy Qualifiers

Security Domain Pty Limited Outsourced User CA policy:

Certificates are issued under this policy to subordinate CAs within the Security Domain Pty Limited PKI, but outsourced to another company to operate at external premises.

SDPL Demo CA Policy Qualifiers

Security Domain Pty Limited Demonstration Certificate Policy: Certificates are issued under this policy for demonstration purposes only. No liability for their use is accepted by Security Domain Pty Limited.

SDPL RA Policy Qualifiers

Security Domain Pty Limited Registration Authority Policy: Certificates are issued under this policy to Registration Authorities known to, or established by Security Domain Pty Limited. Security Domain Pty Limited accepts no liability for the actions of such Registration Authorities.

End User Certificate Policy Qualifiers

Security Domain Pty Limited Standard Certificate Policy: Certificates are issued under this policy to users of Baltimore products whose identity has been established, and verified, by a Registration Authority known to Security Domain Pty Limited. Security Domain Pty Limited accepts no liability for the validity of these Certificates, or for the actions of the issuing Registration Authority or for the actions of the Certificate owner.

1.1.0.4 Other Certificate extensions

Certificates may be issued containing private or service-oriented extensions. Communities of interest may define these extensions to carry information unique to those communities, for example to include additional attributes in an Attribute Certificate.

1.1.0.5 Criticality of Certificate extensions

Certificate extensions are assigned a criticality value of “true” or “false”.

Where the criticality of an extension is:

1. “true”, it is the responsibility of relying parties to understand the purpose of the extension and to be aware of any specific processing requirements, otherwise they should place no reliance on the Certificate;
2. “false”, the relying party must make their own determination of the importance of the information and of the need to be aware of any specific processing requirements.

Key Usage fields in all Certificates issued within the SDPL PKI have a criticality value of “true”.

The purpose and meaning of Certificate extensions are explained in the associated CPS⁽¹⁾.

1.1.3 Definitions

This CPS₍₂₎ assumes that the reader is familiar with basic PKI concepts, including:

1. the use of digital signatures for authentication, integrity and non-repudiation;
2. the use of encryption for confidentiality;
3. the principles of asymmetric encryption, public key Certificates and key pairs;
4. the role of Certification Authorities and Registration Authorities.

Readers wishing further information about PKI should refer to the web sites at:

www.secdom.com.au

www.baltimore.com

Definitions used within this document are contained in Appendix A – Glossary. These definitions are based on:

1. ISO Glossary of IT Security Technology¹; and,
2. GPKA Glossary of Terms².

The definitions differ from these glossaries only in so far as it is necessary for clarity within the framework of the SDPL PKI hierarchy.

1.1.4 X500 Object Identifier hierarchy

Object Identifiers (OID) have been assigned by SDPL and documented in a Configuration baseline.

OIDs are assigned to:

1. the SDPL RCA;
2. each CA and CPS₍₁₎ within the SDPL PKI.

OIDs are not assigned to RAs or AAs, or to this CPS₍₂₎.

All OID are recorded in:

1. an appropriate CPS₍₁₎:
 - the SDPL RCA OID is recorded in each CPS₍₁₎ issued under its hierarchy;
 - a CA's OID is recorded in each CPS₍₁₎ under which it issues Certificates;

¹ Glossary of IT security terminology prepared by JTC1 SC 27 at <http://www.iso.ch:8080/jtc1/sc27/27sd698a.htm>

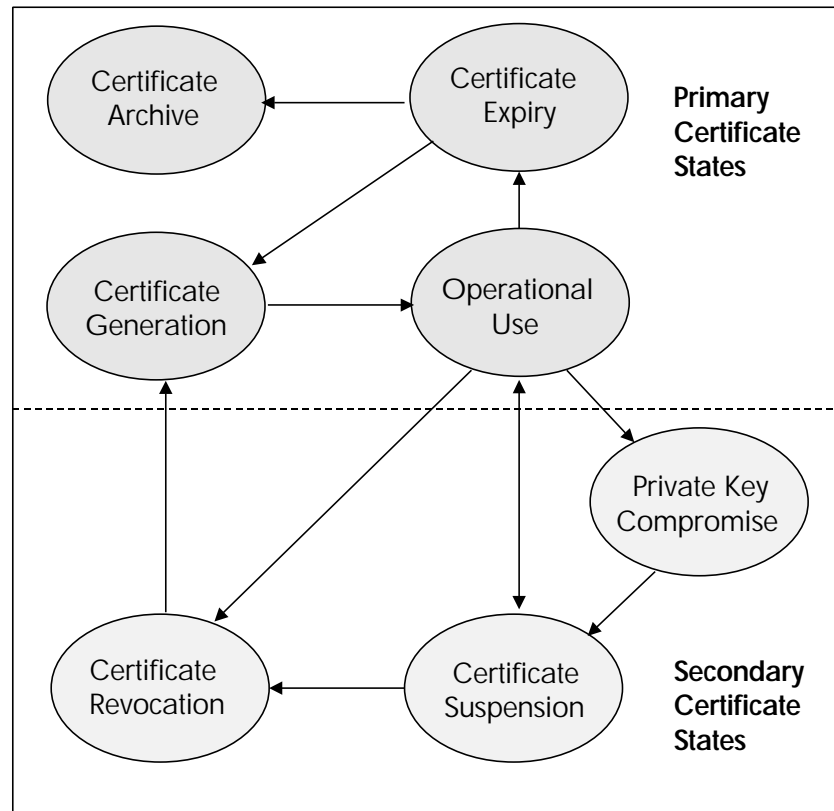
² Government Public Key Authority web site at <http://www.gpka.gov.au/>

- a CPS₍₁₎ OID is recorded in the relevant CPS₍₁₎;
- 2. internal SDPL records.

1.1.5 Certificate Management Life Cycle

The SDPL Certificate Management Life Cycle (CMLC) is illustrated in Figure 1.1 below. The CMLC applies to all Certificates issued within the SDPL PKI.

Figure 1.1 Certificate Management Life Cycle



The CMLC represents the high-level Certificate management process within the SDPL PKI. It consists of primary and secondary Certificate states. The primary states are:

1. generation;
2. operational use;
3. expiry; and
4. archive

All Certificate types issued pass through these three primary states as part of their life cycle.

The secondary states are:

1. compromise;

2. suspension; and,
3. revocation.

Because these secondary states represent exception situations, it is expected that:

1. most End User Certificates will pass through only the primary states during their life cycle;
2. a small number of End User Certificates may pass through one or more of the secondary states.

The SDPL PKI supports the CMLC Certificate states in the delivery of all of its Certificates. It should be noted that some Certificate states may be supported on a procedural basis only.

The CMLC does not support a provisional Certificate state. Certificates are issued after a Certificate application has been submitted and approved, and are deemed to be in operational use in accordance with the CPS₍₁₎.

A complete copy of the CMLC applicable to SDPL CA service provider may be found at:

www.secdom.com.au

www.baltimore.com

Key Pairs

Key pairs are bound to Certificates and are programmed to expire at the same time that the Certificate expires. Key pairs can be registered under more than one Certificate.

Expired key pairs are not re-issued or otherwise re-used.

High level process

The CMLC high level process is outlined in the decision tree illustrated below.

authorised digital Certificate request. Certificate requests are initiated only by approved Registration Authorities (RA).

In making Certificate requests, the RA is contractually bound to:

1. confirm that the user's name does not appear in its list of compromised users;
2. comply with a nominated registration procedure in a CPS₍₁₎ including verification of identification and/or employment;
3. comply with all privacy requirements;
4. obtain approval to make a Certificate request;
5. obtain an acknowledgement that the Certificate Details can be published on a directory service.

Certificate owner names are unique and comply with the X.520 standard for Distinguished Names.

An audit process operates to ensure that SDPL PKI complies with the requirements of the Gatekeeper Accreditation process.

The RA requesting Certificate generation acts as a trusted third party in verifying:

1. the relationship between the key pair and the Certificate owner;
2. the identity and any designated attributes or characteristics of the Certificate owner.

1.1.5.2 Operational use

A Certificate comes into operational use at the time of issue, and remains in operational use until it:

1. expires; or,
2. is compromised, suspended or revoked.

A Certificate that is suspended returns to operational use if the suspension is withdrawn, or if a notice of revocation is not received by the end of the Grace Period.

Certificate lifetimes

Certificates have a fixed operational lifetime that is determined by the SDPL PAA. Subordinate CAs and RAs in the SDPL PKI are only enabled to support specific Certificate profiles including validity date and periods.

The validity period of a Certificate depends on its intended usage and the policy domain within which it is issued. All Certificates are issued with a designated expiry date.

1.1.5.3 Expiry

Certificates expire automatically upon reaching the designated expiry date, at

which time the Certificate is archived.

Note that:

1. the life of a Certificate can not be and is not extended;
2. expired Certificates can not be and are not re-issued.

1.1 .5.4 Archive

Expired Certificates are archived for a minimum period of seven years from the date of expiry, unless another period is specified in the relevant CPS₍₁₎.

1.1 .5.5 Compromise

Certificates in operational use that become compromised are revoked in accordance with a defined procedure. Certificates are deemed to be compromised when the integrity of:

1. the Private key associated with the Certificate is in doubt;
2. the Certificate owner is in doubt, for example they have used, or attempted to use their key pairs for malicious or unlawful purposes.

Consistent with a nominated CPS₍₁₎ Certificates remain in the compromised state for only such time as it takes to arrange for revocation.

1.1 .5.6 Suspension

A Suspension notice warns PKI users that a particular Certificate is under investigation for a limited period of time, known as the “grace period”.

Suspension is used as interim step before revocation is effected and involves issuing a notice to PKI users advising:

1. that a Certificate is under investigation;
2. the period during which the suspension applies.

The Suspension notice appears on a nominated SDPL PKI X.500 Directory. The notice does not set out the reasons for suspension or the results of any investigation. Only the fact of the suspension is provided.

1.1 .5.7 Revocation

Certificate revocation permanently invalidates any trusted use of a Certificate.

Certificates are revoked when:

1. there is a compromise of the Certificate owner’s Private Key;
2. there is a misuse of the Certificate;
3. there is a misrepresentation or errors in the Certificate;
4. the Certificate is no longer required.

Revoked Certificates are added to the SDPL PKI X.500 directories Certificate Revocation List (CRL).

1.1.5.8 Operational compliance

All Certificate operations comply with:

1. the policy requirements of:
 - a recognised Certificate Policy Statement (CPS₍₁₎);
 - this CPS₍₂₎;
 - published and internal privacy policies and practices;
 - published and internal security policies and practices;
2. the technology requirements of:
 - relevant internal guidelines for the physical protection of technology assets;
 - X.500 Directory services;
 - X.509 Certificate format;
 - X.509 Certificate Revocation List (CRL) format;
 - X.500 Distinguished name standards;
 - PKCS#7 format for Digital Encryption and Digital Signatures;
 - PKCS#10 Certificate Request format;
 - recognised PKI conventions and standards;
3. legal requirements of domestic and, where applicable, international privacy legislation;
4. appropriate international and domestic standards relevant to PKI operations;
5. audit requirements for Certificate operations.

1.1.6 PKI Operational Infrastructure

The SDPL PKI operational infrastructure:

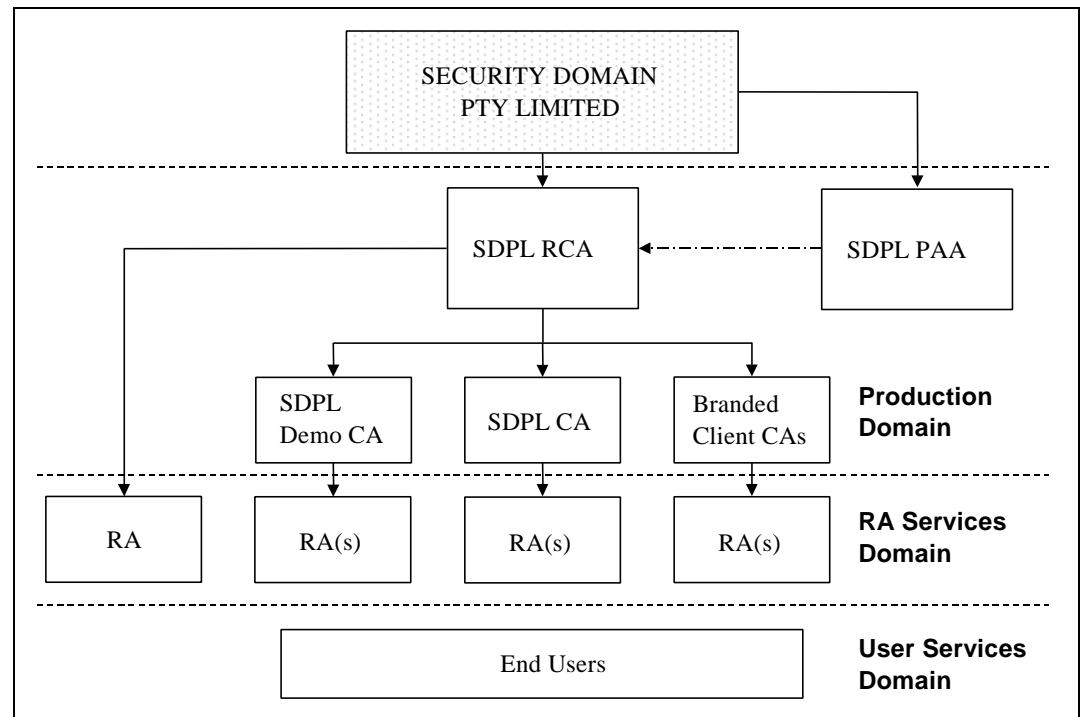
1. uses products from Baltimore. These products automate key and Certificate management functions;
2. employs a common architectural model under which Certification and Registration functions are separated.

The SDPL PKI operational infrastructure comprise three distinct domains:

1. Production Domain;
2. RA Services Domain;
3. User Services Domain.

Figure 1.3 below provides a diagrammatical representation of these domains, which is followed by explanatory text.

Figure 1.3 SDPL PKI Operational Infrastructure



Production domain

The hierarchy in the Production Domain consists of the SDPL RCA and all CAs that are operated by SDPL on its own site. The RCA establishes and maintains the PKI while the CAs are responsible for issuing Certificates.

There are two types of CA within this domain:

1. CAs managed by SDPL ("SDPL CAs");
2. CAs managed by clients ("Branded Client CAs").

RA service domain

The RA Services Domain consists of all RAs that are operated under the SDPL hierarchy. These RAs are responsible for supplying user registration and key generation services to End Users.

User service domain

The User Services Domain includes End Users, who use or rely on Certificates for authentication, integrity non-repudiation and confidentiality.

1.1.6.1 Validation of digital signatures

The End User product selected for use within and supported the SDPL PKI provides the following functions automatically:

1. verification that the digital signature has been created by the private key bound to the Certificate listed for the signing party in the SDPL X.500 Directory;
2. a mechanism by which the message, transaction or other file (“signed file”) may be checked to determine that it has not been altered since the digital signature was appended.

The End User product can accomplish these automatic functions by:

1. establishing a Certificate chain³ for validation of the signature, commencing with the signing party’s Certificate and ending with the RCA’s Certificate. Note that it is possible to establish more than one Certificate chain for a signature, through cross-certification.
2. where more than one Certificate chain can be established, the End User product can be utilised to:
 - allow the End User various options to manually establish the chain; or,
 - establish a chain through a series of user-defined preferences; or,
 - establish the shortest possible chain; or,
 - validate all possible chains.
3. validating all Certificates in the established chain(s);
4. using the signing party’s public key to apply a hash function to the signed file;
5. comparing the resulting hash to the hash that is appended to the signed file, produced using the signing party’s private key.

The End User is able to verify:

1. the validity of the transaction, by inspecting the signing party’s CPS₍₁₎ to ensure the signing party has acted:
 - in a valid and authorised manner in terms of the Certificate usage allowed by the CPS₍₁₎;
 - in compliance with any special requirements of the CPS₍₁₎.
2. at their own discretion whether the Certificate has been revoked, by checking the CRL in the X.500 Directory.

³ A list of certificates, typically commencing with an End User Certificate, then progressing to the Certificates of: the End User’s RA, the issuing CA, and the RCA.

1.1.7 Scope

The practices described in this CPS₍₂₎ are:

1. based upon but not limited to, the roles, responsibilities, duties and obligations contained within SDPL Standard CPS₍₁₎ for Individuals, Organisations and Employees;
2. binding upon all parties within the SDPL PKI, through the inter-linking contractual responsibilities, obligations and duties between:
 - the SDPL RCA and its subordinate CAs;
 - CAs and their subordinate RAs;
 - RAs and their registered End Users.

This CPS₍₂₎ incorporates information from other documents regarding practices involved in the issue, use and validation of Certificates, and in the operational maintenance of the PKI infrastructure. It includes, but is not limited to the:

1. Certificate categories that may be created;
2. establishment of Service Providers;
3. functions and obligations of Service Providers;
4. registration of End Users;
5. functions and obligations of End Users;
6. process of approving new Certificate categories and Certificate policy.

1.1.8 Security Philosophy

The security philosophy governing the operational management of the SDPL PKI is:

“Prevention, Detection and Considered Response”.

‘Considered response’ describes the execution of such actions as are justified having considered all the circumstances.

This philosophy means that the first aim of a Service Provider is:

1. to prevent any unauthorised action taking place;
2. should an unauthorised action take place, to be able to detect and record the unauthorised event or action;
3. finally, to respond to unauthorised events or actions in a considered and positive manner.

In all cases, SDPL Service Providers operate to:

1. securely generate their private keys and take adequate precautions to protect against their compromise, modification, disclosure, loss or unauthorised use;
2. be able to detect and record unauthorised events and actions.

1.1.9 Staffing Arrangements

The SDPL PKI has adopted and employs personnel and management practices to ensure the trustworthiness, integrity and professional conduct of its staff. The personnel standards described below are applied.

All SDPL operations staff:

1. are vetted to assess their suitability;
2. enter into non-disclosure agreements to protect against the unauthorised disclosure of confidential information;
3. are trained in:
 - basic PKI concepts;
 - the use and operation of CA or RA software;
 - documented CA or RA procedures;
 - computer security awareness and procedures;
 - for pertinent CA staff, how to explain to RA certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
 - for pertinent RA staff, how to explain to End User certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
 - the meaning and effect of the legal contract their service provider has signed with its superior entity;
 - the meaning and effect of relevant CPS₍₁₎, this CPS₍₂₎ and for pertinent RA staff, the subscriber agreement.

1.1.10 Rights of Investigation

The SDPL RCA reserves the right through contract, CPS₍₁₎ and operational doctrine to:

1. investigate to the fullest extent possible under the law, the circumstances behind any:
 - compromise or suspected compromise of any private key in its chain of trust;
 - any non-compliance, or suspected non-compliance with the practices

prescribed in a service provider operating agreement, a relevant CPS₍₁₎ or this CPS₍₂₎.

2. take such actions as it considers justified having considered the findings of its investigation.

The RCA's investigation of a service provider may include, but is not limited to:

1. interviews with operational or corporate staff;
2. a review of pertinent system logs, operational records and other related files or documents including e-mail messages;
3. an audit of operational procedures;
4. an audit of security controls, procedures and measures;

An investigation may include, but is not limited to:

1. interviews;
2. requests for information;
3. requests for the production of nominated documents or system logs.

1.1.10.1 CA rights

CAs have identical rights of investigation in relation to parties beneath them in the chain of trust.

1.1.10.2 RA rights

RAs have identical rights of investigation in relation to the compromise or suspected compromise of Private Keys belonging to parties beneath them in the chain of trust.

Refer also to 2.6.3 *Compliance Audit*.

1.2 Identification

This CPS₍₂₎ is referred to as the "Security Domain CPS₍₂₎".

Object Identifiers (OID) are not applicable to CPS₍₂₎ documents.

1.3 Community and Applicability

SDPL has established a Root Certification Authority (RCA) under which a number of subordinate CAs and RAs operate.

These subordinate CA or RA services within the SDPL PKI are either:

1. managed and operated by SDPL; or,
2. managed by clients but operated by SDPL (outsourced services); or,

3. managed and operated by clients (external services).

This CPS₍₂₎ supports:

1. all CA and RA services that operate under the SDPL RCA, i.e. that are within the SDPL “chain of trust”;
2. all Standard Certificates issued under the SDPL RCA hierarchy.

As a consequence, the practices described in this document allow for a wide range and variety of:

1. Certificate types, supporting individual transactions that have differing levels of information sensitivity and financial value;
2. End Users, who may include:
 - individuals;
 - commercial or non-profit organisations;
 - departments, agencies or authorities of a country’s State or National Government (excepting Australia and New Zealand);
3. CA and RA service operators.

The practices in this CPS₍₂₎:

1. accommodate the diversity of the community and the scope of applicability within the SDPL chain of trust;
2. adhere to the primary purpose of the CPS₍₂₎, of ensuring the uniformity and efficiency of practices throughout the PKI.

In keeping with their primary purpose, the practices in this document:

1. are the minimum requirements necessary to ensure that subscribers and relying parties have the highest possible level of assurance, and that critical functions are provided at appropriate levels of trust;
2. apply to all stakeholders, for the generation, issue, use and management of all Certificates and key pairs.

1.3.0 Policy Authorities

1.3.0.1 Security Domain Pty Limited Policy Approval Authority (SDPL PAA)

The SDPL PAA has been established to maintain the integrity of the policy infrastructure in the SDPL PKI.

1.3.0.2 SDPL PAA functions

The SDPL PAA performs the following functions:

1. CPS₍₁₎ approval within the SDPL PKI;
2. ensure the integrity of PKI policy structures.

1.3.0.3 SDPL PAA Contact Details

The contact details for the SDPL PAA are published in each CPS₍₁₎ within the SDPL hierarchy.

1.3.0.4 Policy Creation Authorities (PCA)

PCA are responsible for formulating policy relating to a specific part of the SDPL PKI, for example for Certificates issued by a specific CA.

Within the SDPL PKI, the PCA function is carried out directly by the SDPL PAA.

1.3.0.5 PCA functions

The PCA performs the following functions:

1. formulate new policy and policy changes within the SDPL PKI;
2. submit new or changed policies to the SDPL PAA for approval.

1.3.0.6 PCA Contact Details

The contact details for the SDPL PAA are published in each CPS₍₁₎ within the SDPL hierarchy.

1.3.1 Certification Authorities

1.3.1.1 SDPL Root Certification Authority

The SDPL RCA is the highest point of trust within the SDPL PKI hierarchy. The primary purpose of the RCA is to certify subordinate Certification Authorities (CA), by digitally signing their Certificates. The SDPL RCA self-signs its own Certificate.

The RCA is accessed via a single Registration Authority (RA) which is used solely for the purpose of creating subordinate CA Certificates.

The key length of the SDPL RCA's Signing Key, used to sign Certificates, is as determined by a relevant Certificate profile. Generation of the RCA's keys is performed on a platform in a physically secure facility.

1.3.1.2 SDPL RCA Functions

The functions performed by the SDPL RCA include:

1. constitution of a PAA for the purpose of reviewing and approving policies applicable to and recognisable by, the RCA;
2. generation of its own keys;
3. issuing a self signed Certificate;
4. publication of its Public Key Certificate in the SDPL X.500 Directory services;
5. providing relying parties with access to:
 - Certificate information published in the directory services;
 - the public keys associated with operational Certificates that are listed in the directory services;
6. publication of its Root CA Hash on the web sites at:

www.secdom.com.au

www.baltimore.com

7. operation of the RCA in an efficient and trustworthy manner and in accordance with:
 - the RCA CONOPS;
 - the SDPL Standard CPS₍₁₎ for Individuals, Organisations and Employees;
 - this CPS₍₂₎;
 - SDPL security policies;
 - documented operational procedures;
8. approve the naming conventions for the creation of distinguished names for Certificate applicants, in compliance with the X.520 standard for Distinguished Names;
9. administration of the registration of subordinate CAs;
10. issuance of Certificates for subordinate CAs on the receipt of authenticated digitally signed certification requests;
11. publication of issued Certificates in the SDPL X.500 Directory services;
12. investigation of compromises and suspected compromises of private keys at any level it deems warranted in its chain of trust;

13. revocation of Certificates on receipt of authenticated digitally signed revocation requests, or when deemed warranted following its investigation of the compromise or suspected compromise of a private key;
14. posting revoked Certificates in the directory services CRL;
15. conduct of regular internal security audits;
16. conduct of compliance audits of immediately subordinate CAs when Certificate renewal is due.

1.3.1.3 SDPL RCA Contact Details

The contact details for the SDPL RCA are described and published in each CPS₍₁₎ within the SDPL hierarchy.

1.3.1.4 Certification Authorities

The primary purpose of the various CAs operating under the SDPL hierarchy is to provide Certificate management services (generation, operational use, compromise, suspension, revocation and expiry) for End Users within their respective policy domain(s). These CAs consist of:

1. the SDPL CA, that provides Certificate management services for customers who do not wish to operate their own Certification Authority;
2. branded client CAs, that operate under a customer's name but are maintained and supported by SDPL;
3. CAs that are operated by customers on their own sites.

The key length of a CA's:

1. CA Key, used to sign Certificates is as determined by a relevant Certificate profile;
2. Protocol Key, used to sign responses to RA requests is as determined by a relevant Certificate profile.

Typically the key length for a CA or Protocol key is 1024 bits.

Generation of the CA's keys is performed on a platform in a physically secure facility.

1.3.1.5 CA Functions

CAs operating under the SDPL hierarchy perform the following functions:

1. generate their own keys;
2. submit their public keys together with digitally signed certification requests to the SDPL RCA;
3. publish each CPS₍₁₎ under which they issue Certificates, and this CPS₍₂₎ on a nominated web site specified within a relevant CPS₍₁₎. The SDPL CA publishes relevant CPS₍₁₎ and this CPS₍₂₎ on:

www.secdom.com.au

www.baltimore.com

4. operate the CA in an efficient and trustworthy manner and in accordance with:
 - the SDPL PKI CONOPS;
 - an RCA-CA agreement (note that an RCA-CA agreement, which is a contractual document, does not exist between the SDPL RCA and the SDPL CA, which are the same legal entity);
 - all CPS₍₁₎ that they issue Certificates under;
 - this CPS₍₂₎;
 - SDPL or internal security policies;
 - documented operational procedures;
5. on the receipt of authenticated digitally signed Certificate requests from authorised Registration Authorities, issue Certificates in accordance with the associated CPS₍₁₎ for:
 - RAs;
 - End Users;
6. publish issued Certificates in a nominated X.500 Directory. The SDPL CA publishes these Certificates in the SDPL X.500 Directory;
7. investigate compromises and suspected compromises of private keys at any subordinate level they deem warranted in their chain of trust;
8. revoke Certificates on receipt of authenticated digitally signed revocation requests, or when deemed warranted following their investigation of the compromise or suspected compromise of a private key;
9. post revoked Certificates in the directory services CRL;
10. conduct regular internal security audits;
11. conduct compliance audits of subordinate RAs when Certificate renewal is due;
12. assist in audits conducted by the RCA to validate the renewal of their own Certificates.

1.3.1.6 CA Contact Details

The contact details for the CAs that operate under the SDPL hierarchy are

published in each CPS₍₁₎ that they issue Certificates under, or the CPS₍₁₎ may advise a web site address or other location where the contact details may be found.

1.3.2 Registration Authorities

The primary purpose of an RA is to register End Users. RAs have the responsibility of accepting Certificate applications, authenticating the identity or other credentials of the applicant, then approving or rejecting the application. These obligations are enforced in contract and are set out in a set of RA operating procedures.

Each RA within the SDPL hierarchy is subordinate to a nominated CA, this is a function of the operating hierarchy.

The key length of an RA's:

1. Authentication key, used to sign requests to a nominated CA is as determined by a relevant Certificate profile.
2. Confidentiality key, used for receiving encrypted messages, is as determined by a relevant Certificate profile.

The generation of an RA's keys is performed on a platform in a physically secure facility.

1.3.2.1 RA Functions

RAs perform the following functions:

1. generate their own keys;
2. submit their public keys together with digitally signed certification requests to their superior CA;
3. operate the RA in an efficient and trustworthy manner and in accordance with:
 - the RCA CONOPS;
 - a CA-RA agreement (note that a CA-RA agreement, which is a contractual document, does not exist between CAs and RAs that are the same legal entity, for example, the SDPL CA and SDPL RA);
 - each CPS₍₁₎ that it accepts Certificate applications under;
 - this CPS₍₂₎;
 - its internal security and privacy policies;
 - documented operational procedures.
4. register End Users including:
 - authenticating material Certificate information, such as sighting Proof of Identity (POI) documentation;
 - proposing and approving distinguished names for Certificate applicants;

- confirming that a Certificate applicant's name does not appear in their list of compromised users;
 - generating key pairs for Certificate applicants, or accepting End User generated keys provided the End User can both prove possession of and establish their right to use the key pairs;
 - obtaining a subscriber agreement;
5. submit End User public keys together with digitally signed certification requests to their superior CA, and receive the Certificates issued in accordance with these requests;
 6. issue keys and Certificates to End Users, ensuring that private keys and PICs are not obtained by third parties prior to being received by the End User, and that private keys are not captured by any other mechanism under the control of the RA;
 7. authenticate requests from End Users for the renewal or revocation of their Certificates, and generate digitally signed renewal or revocation requests to their superior CA;
 8. may notify End Users of the imminent expiry of their Certificates. Where such a service is provided, End Users are not to rely upon the RA's notification but are to retain sole responsibility for requesting Certificate renewal before the expiry of their current Certificates;
 9. investigate compromises and suspected compromises of private keys at any subordinate level they deem warranted in their chain of trust;
 10. initiate Certificate revocation when deemed warranted following their investigation of the compromise or suspected compromise of a private key;
 11. maintain a list of compromised keys and compromised users and periodically provide these lists to their superior CA;
 12. conduct regular internal security audits;
 13. assist in audits conducted by their superior CA to validate the renewal of their own Certificates.

1.3.2.2 RA Contact Details

The contact details for RAs that operate under the SDPL hierarchy are published in each CPS₍₁₎ that they issue Certificates under, or the CPS₍₁₎ may publish a web site address or other location where the contact details may be found.

1.3.3 End Entities

End Users may be natural persons, commercial, non-profit or sporting organisations or national or state government departments, agencies or authorities.

An End User acts as a subscriber when they use their keys to encrypt and/or digitally sign a message, transaction or other electronic file.

An End User acts as a relying party when they rely on another user's public keys to decrypt and/or authenticate a message, transaction or other electronic file.

The key length of an End User's Authentication and Confidentiality keys is determined by a relevant Certificate profile and is specified in the relevant CPS⁽¹⁾.

Where End User key pairs are generated by:

1. RAs, generation is to be performed on a platform in a physically secure facility;
2. End Users, reasonable security measures are to be taken to ensure the protection of their private keys against compromise.

1.3.3.1 End Entity Functions

End Users perform the following functions:

1. request the issue, renewal and if appropriate, revocation of their Certificates;
2. generate key pairs where the keys associated with a Certificate request are End User generated;
3. use their keys and Certificates in a manner and for a purpose consistent with the requirements of the associated CPS⁽¹⁾ and the practices in this CPS⁽²⁾;
4. rely on operational Certificates for the authentication and/or decryption of messages, transactions or other files;
5. regularly check the X.500 Directory services CRL to determine whether a Certificate they are relying on has been revoked.

1.3.3.2 End User Contact Details

The following End User contact details may be published in an End User's Public Key Certificate in compliance with X.509 standards:

1. organisation name and department name in the End User's Distinguished Name in the Subject field;
2. the End User's e-mail address, or Universal Resource Location (URL) may be published in the Subject Alternative Name field.

End User contact details are maintained by the End User's RA.

1.3.4 Applicability

Certificates issued by the SDPL RCA are used to support secure electronic commerce and the secure exchange of information by electronic means:

1. globally, with the exception of Australia, its Territories and New Zealand;
2. between government bodies, business, charitable bodies, professional organisations, strata schemes, sporting associations, community bodies, special interest groups, registered clubs and private individuals in any combination;

3. within both closed and open PKI communities.

The practices described in this CPS₍₂₎ support a large, diverse and widespread community of users who require PKI certificate services in support of electronic transactions and information services.

The SDPL PKI user community may regard the practices described in this CPS₍₂₎ as:

1. ensuring standard operating procedures and uniform quality of service delivery across the PKI;
2. fostering and promoting high levels of trust and integrity across the PKI.

1.3.4.1 **Applicable Certificate usage**

The SDPL RCA supports a variety of functional classes. Typically Certificates supported by this CPS₍₂₎ fall into one or more of the primary functional classes set out below:

1. "Identity" Certificates;
2. "Financial" Certificates;
3. "Attribute" Certificates;
4. "Functional" Certificates.

Within each of these classes, different assurance levels apply, or different attributes are used.

SDPL Standard Certificates may encompass all of the abovementioned Certificate classes. Within nominated policy domains, Certificates may also be used for multiple purposes.

Table of functional Certificate classes

Class	Purpose	Assurance levels
Identity	Authenticates Certificate holder's identity through a rigorous POI process.	Low, medium and high.
Financial	Authorises Certificate holder to initiate financial transactions of a certain type and limit.	Low, medium and high.
Attribute	Associates Certificate holder with pre-defined access rights and system privileges.	Not applicable as levels of access, etc. are defined within Certificate attributes.
Functional	Identifies Certificate holder's function or role.	Low, medium and high.

1.3.4.2 Identity Certificates

Identity Certificates authenticate the identity of the person or organisation to whom they are issued. Designated uses include:

1. within messaging systems, to authenticate the identity of a person or organisation sending a message and to provide assurance that subsequent communications are from the same person or organisation;
2. in secure electronic data exchange, to authenticate and protect sensitive information.

The criteria used by a registrar for the authentication of a Certificate owner's identity depend upon:

1. the type of Certificate, i.e. individual, organisation or employee;
2. the grade of certificate, i.e. low, medium or high assurance level.

1.3.4.3 Financial Certificates

Financial Certificates are issued to authorise and verify a range of financial transactions to a given monetary limit and for designated purposes.

1.3.4.4 Attribute Certificates

Attribute Certificates bind the Certificate owner to one or more attributes associated with the Certificate owner. Designated uses include:

1. the Certificate owner's relationship with an organisation;
2. logon rights or directory privileges associated with the Certificate Owner;
3. the role of an individual or other entity.

1.3.4.5 Functional Certificates

Functional Certificates are issued to entities including but not limited to individuals and organisations, to facilitate the performance of a specific function or group of functions. Designated uses include functional Certificates issued to facilitate:

1. the automatic processing of transactions by a file server;
2. the provision of certification services by SDPL PKI service providers.

1.3.4.6 Restricted Certificate usage

Specific restrictions on the use of a Certificate are contained in the CPS⁽¹⁾ under which the Certificate is issued. These restrictions may limit or prescribe the:

1. community of interest;
2. conditions which must be satisfied before a Certificate is used;

3. actual usage of the Certificate;
4. processing steps or other actions which are to be performed after a Certificate has been used.

Parties within the SDPL PKI are to use Certificates only in the manner, and for the purposes prescribed in a relevant CPS₍₁₎. Any use of a Certificate in a manner or for a purpose not in accordance with a relevant CPS₍₁₎ is not recognised nor supported by this CPS₍₂₎.

1.4 Contact Details

1.4.1 Specification administration organization

This CPS₍₂₎ is administered by Security Domain Pty Limited.

1.4.2 Contact person

Enquiries or other communications about this document should be addressed to:

**General Manager -
Certificates On-Line
Security Domain Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
2060 AUSTRALIA**

E-mail may be sent to:

info@secdom.com.au

1.4.3 Specification administration organization

This CPS₍₂₎ is administered by Certificates Australia Pty Limited.

1.4.4 Contact person

Enquiries or other communications about this document should be addressed to:

**General Manager -
Certificates On-Line
Security Domain Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
2060 AUSTRALIA**

E-mail may be sent to:

info@secdom.com.au

1.4.5 Person determining CPS suitability for this policy

See 1.4.2 *Contact person*.

2. GENERAL PROVISIONS

2.1 Obligations

Certificate owners are:

1. advised through the CPS₍₁₎ of their duties and obligations to ensure the safety, protection and integrity of their private keys;
2. required for specific classes of Certificates to enter into an agreement that clearly defines these obligations;
3. not to interfere with or damage, or attempt to interfere with or damage, the operational infrastructure of the SDPL PKI or any component thereof. The SDPL PKI has:
 - been structured and is operated in such a manner as to minimise the risk of compromise or willful damage by a Certificate owner;
 - defined a security policy that provides for the early detection of an attempt to damage the infrastructure and to collect sufficient evidence for a prosecution.

2.1.0 SDPL Obligations

2.1.0.1 SDPL PAA Obligations

The SDPL PAA has no Certificate practice obligations under this CPS₍₂₎. The SDPL PAA's general obligations in regard to approving CPS₍₁₎ and maintaining the SDPL PKI policy infrastructure are detailed in a relevant CPS₍₁₎.

2.1.0.2 RCA Obligations

The SDPL RCA discharges its obligations under this CPS₍₂₎ by:

1. providing the SDPL PKI operational infrastructure and certification services, including X.500 Directory and service provider software;
2. making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit the RCA to operating in compliance with:
 - documented operational procedures;
 - this CPS₍₂₎;
 - within applicable law;
3. approving the establishment of all new CAs at any level in the SDPL hierarchy and on approval, executing an RCA-CA operating agreement;

4. maintaining this CPS₍₂₎ and enforcing the practices described within it;
5. publishing its Root CA Hash on the Security Domain web site and other nominated web sites;
6. issuing Certificates to authorised CAs, that comply with X.509 standards and are suitable for the purpose required;
7. issuing Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
8. publishing issued Certificates without alteration in the X.500 Directory;
9. investigating any suspected compromise which may threaten the integrity of the PKI;
10. revoking Certificates in terms of section 4.4.1 - *Circumstances for revocation* and post such revoked Certificates in the X.500 Directory CRL;
11. promptly notifying Certificate owners in the event it initiates revocation of their Certificates;
12. conducting compliance audits of immediately subordinate CAs when Certificate renewal is due.

2.1.1 CA Obligations

CAs operating under the SDPL hierarchy discharge their obligations under this CPS₍₂₎ by:

1. making reasonable efforts to ensure they conduct an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit the CA to operating in compliance with:
 - an RCA-CA agreement (note that an RCA-CA agreement, which is a contractual document, does not exist between the SDPL RCA and the SDPL CA, which are the same legal entity);
 - documented operational procedures;
 - applicable CPS₍₁₎;
 - this CPS₍₂₎;
 - within applicable law;
2. approving the establishment of subordinate RAs and on approval, executing a CA-RA operating agreement (note that a CA-RA agreement, which is a contractual document, does not exist between CAs and RAs that are the same legal entity, for example, the SDPL CA and SDPL RA);
3. enforcing within the sphere of their operations the practices described within this CPS₍₂₎;
4. publishing applicable CPS₍₁₎ and this CPS₍₂₎ on the web site(s) nominated in the

CPS₍₁₎;

5. upon receipt of a valid Certificate request, issuing Certificates which comply with X.509 standards and meet the requirements of the request;
6. issuing Certificates that are factually correct from the information known to them at the time of issue, and that are free from data entry errors;
7. publishing issued Certificates without alteration in a nominated X.500 Directory;
8. investigating any suspected compromise which may threaten the integrity of the PKI at any subordinate level within its chain of trust;
9. revoking Certificates in terms of section 4.4.1 - *Circumstances for revocation* and posting such revoked Certificates in the X.500 Directory CRL;
10. promptly notifying Certificate owners in the event the CA initiates revocation of a Certificate;
11. maintaining a list of compromised keys and compromised users. The compromised list is to include relevant information regarding the identity of the individual(s) or organisation(s) concerned, reasons and causes for inclusion on the list and such other information as might be required to minimise damage or liability to all SDPL End Users;
12. conducting compliance audits of immediately subordinate CAs and RAs when Certificate renewal is due;
13. assisting in audits conducted by the RCA to validate the renewal of their own Certificates.

2.1.2 RA Obligations

RAs operating under the SDPL hierarchy discharge their obligations under this CPS₍₂₎ by:

1. making reasonable efforts to ensure they conduct an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit the RA to operating in compliance with:
 - a CA-RA agreement (note that a CA-RA agreement, which is a contractual document, does not exist between CAs and RAs that are the same legal entity, for example, the SDPL CA and SDPL RA);
 - documented operational procedures;
 - applicable CPS₍₁₎;
 - this CPS₍₂₎;
 - within applicable law;
2. enforcing within the sphere of their operations the practices described within this CPS₍₂₎;

3. accepting End User Certificate applications, including authenticating material Certificate information, obtaining a subscriber agreement and accepting or rejecting the application;
4. where required, archiving private confidentiality keys they have generated;
5. verifying the integrity and possession of, and establishing the End User's right to use, user generated keys presented for certification;
6. advising End Users of their obligations under the relevant CPS₍₁₎, this CPS₍₂₎ and the appropriate subscriber agreement, and providing End Users with copies of the relevant CPS₍₁₎ and this CPS₍₂₎ or advising them how these documents may be accessed;
7. submitting Certificate requests that comply with X.509 standards and meet the requirements of approved Certificate applications;
8. submitting Certificate requests that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
9. issuing keys and Certificates to End Users and ensuring that the private keys and key transport access control mechanisms are not obtained by third parties prior to being received by the End User, and that private keys are not captured by any other mechanism under the control of the RA;
10. investigating any suspected compromise which may threaten the integrity of the PKI at any subordinate level within its chain of trust;
11. revoking Certificates in terms of section 4.4.1 - *Circumstances for revocation*;
12. promptly notifying Certificate owners in the event it initiates revocation of their Certificates;
13. maintaining a list of compromised keys and compromised users. The compromised list is to include relevant information regarding the identity of the individual(s) concerned, reasons and causes for inclusion on the list and such other information as might be required to minimise damage or liability to all SDPL End Users;
14. keeping such registration records as may be required;
15. assisting in audits conducted by the SDPL CA to validate the renewal of its own Certificates.

2.1.3 Subscriber Obligations

End Users discharge their obligations under this CPS₍₂₎ by:

1. providing their RA with true and correct information at all times;
2. providing sufficient proof of material Certificate information to meet user registration or Certificate renewal requirements;
3. requesting generation of End User keys or requesting acceptance of self generated keys;

4. proving possession of and establishing their right to use, self-generated keys;
5. acknowledging that in making a certificate application, they are consenting to Certificate issue in the event the application is approved;
6. agreeing to their public keys and Certificates being published in the SDPL directory services as part of Certificate issue;
7. signing a subscriber agreement where required by a relevant CPS₍₁₎;
8. immediately notifying their RA of any error or defect in their Certificates, or of any subsequent changes in the Certificate information;
9. reading the applicable CPS₍₁₎ and this CPS₍₂₎ before using their key pairs;
10. using their keys pairs and other End User's public keys only in accordance with a relevant CPS₍₁₎;
11. ensuring the safety and integrity of their private keys, including:
 - controlling access to the computer containing their private keys;
 - protecting the access control mechanism used to access their private keys;
12. immediately notifying their RA of any instance in which a key pair is compromised or in which they have reason to believe a key pair may have become compromised;
13. exercising due diligence and reasonable judgement before deciding to rely on a digital signature, including whether to check on the status of the relevant Certificate;
14. regularly enquiring on the status of Certificates, by checking the CRL.

2.1.4 Relying party obligations

Relying parties have no Certificate practice obligations under this CPS₍₂₎. Relying parties may however be required under a relevant CPS₍₁₎ to complete a relying party agreement that may contain defined duties, responsibilities or obligations.

2.1.5 Repository Obligations

The SDPL Repository functions are performed by the X.500 Directory.

The SDPL RCA provides and maintains the operational infrastructure for the X.500 Directory, and CAs operating under the SDPL RCA post Certificates and CRLs to the Directory.

Repository obligations are therefore incorporated into sections 2.1.0.2 *RCA Obligations* and 2.1.1 *CA Obligations*.

2.2 Liability

SDPL has introduced a number of measures to reduce or limit its liabilities in the

event that the safeguards in place to protect its resources fail to:

1. inhibit misuse of those resources by authorised personnel;
2. prohibit access to those resources by unauthorised individuals.

These measures include but are not limited to:

1. identifying contingency events and appropriate recovery actions in a Contingency & Disaster Recovery Plan;
2. performing regular system data backups;
3. performing a backup of the current operating software and certain software configuration files;
4. storing all backups in secure local and offsite storage;
5. maintaining secure offsite storage of other material needed for disaster recovery;
6. periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
7. periodically reviewing its Contingency & Disaster Recovery Plan, including the identification, analysis, evaluation and prioritisation of risks;
8. periodically testing uninterrupted power supplies.

2.2.0 SDPL Liability

Limitations upon and the extent of the liability of Security Domain Pty Limited:

1. may vary;
2. are described within relevant contractual documents.

2.1.0.1 SDPL PAA Liability

Limitations upon and the extent of the liability of the SDPL PAA:

1. may vary;
2. are described within relevant contractual documents.

2.1.0.2 SDPL RCA Liability

Limitations upon and the extent of the liability of the SDPL RCA:

1. may vary;
3. are described within relevant contractual documents.

2.2.1 CA Liability

Limitations upon and the extent of the liability of CAs operating under the SDPL hierarchy:

1. may vary;
2. are described within relevant contractual documents.

2.2.2 RA Liability

Limitations upon and the extent of the liability of RAs operating under the SDPL hierarchy:

1. may vary;
2. are described within relevant contractual documents.

2.2.3 End Entity Liability

Limitations upon and the extent of the liability of an End User:

1. may vary;
2. are described within relevant contractual documents.

2.3 Financial responsibility

2.3.1 Indemnification by relying parties

Relying party liability is defined by relevant contractual documents and section 2.4.1 *Governing Law*.

2.3.2 Fiduciary relationships

Issuing certificates, or assisting in the issue of certificates in accordance with this CPS₍₂₎ does not make Security Domain Pty Limited, the SDPL RCA, or CAs or RAs operating under the SDPL RCA an agent, fiduciary, trustee, or other representative of subscribers or relying parties.

2.3.3 Administrative processes

The scope of this CPS₍₂₎ does not include commercial issues such as the financial viability or stability of SDPL customers who operate CA services under the SDPL RCA, other than as provided for in section 4.9 *CA Termination*.

2.3.4 Security Domain Pty Limited

Security Domain Pty Limited is a wholly owned subsidiary of Baltimore. Baltimore is a publicly listed company on the London stock exchange.

2.3.5 Client managed CA and RA services

SDPL clients who manage CA and/or RA services within the SDPL PKI may be requested by Security Domain to provide supporting documentation during initial registration. Clients can assist by providing any reasonable information or documentation required, including information that is classified as being “commercial in confidence”.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

This CPS₍₂₎ is governed by the laws in force in New South Wales, Australia. In addition to this, it is reliant upon a contractual structure from the RCA to the End User.

2.4.1.1 Applicable contract structure

The contractual structure that underpins the practices described in this document include the:

RCA - CA Operating Agreement: Describes contractual arrangements under which SDPL will enable a subordinate outsourced CA and includes the roles and responsibilities of each party. As part of this document, SDPL shall provide a copy of the Concept of Operations document.

CA - RA Operating Agreement: Describes contractual arrangements under which SDPL will enable a subordinate outsourced RA and includes the roles and responsibilities of each party.

Product Licencing Agreement: Describes the licence terms and conditions of products sold to SDPL customers and which are operated in conjunction with a SDPL CA Service Provider’s services.

Customer Agreement: Describes the contractual arrangements between the customer and the SDPL Service Provider. This would include specific arrangements such as: services, service levels, etc.

Subscriber Agreement: Establishes a contractual relationship between RAs and their End Users for the provision of services by the RA.

2.4.2 Severability, survival, merger, notice

2.4.2.1 Severability

In the event that any one or more of the provisions of this CPS₍₂₎ shall for any reason be held to be invalid, illegal, or unenforceable at law, such unenforceability shall not affect any other provision, but this CPS₍₂₎ shall then be construed as if such unenforceable provision or provisions had never been contained herein, and insofar as possible, construed to maintain the origin intent of the CPS₍₂₎.

2.4.2.2 Survival (Continuing obligations)

This CPS₍₂₎ shall be binding upon, and inure to the benefit of all parties hereto. The rights and obligations detailed in this CPS₍₂₎ are not assignable by the parties.

2.4.2.3 Merger

If the private key corresponding to the public key that is specified in a certificate to which this CPS₍₂₎ applies is compromised or the expiration date of a certificate to which this CPS₍₂₎ applies is reached or passed then all rights and obligations except those which are identified in 2.4.2.2 shall merge.

2.4.2.4 Notice

A notice, consent, request or any other communication required under the practices described in this CPS₍₂₎ shall be in a form approved by a relevant CPS₍₁₎.

A notice, consent, request or any other communication is deemed to be received at the time and under the conditions prescribed by a relevant CPS₍₁₎.

2.4.2.5 Notice action

Notices are issued in accordance with relevant CPS₍₁₎.

2.4.2.6 Notice acknowledgement

Specific acknowledgement is not required except as otherwise provided for within these practices and a relevant CPS₍₁₎.

2.4.3 Dispute resolution procedures**2.4.3.1 Hierarchy of Certificate policy**

In the event of a conflict between this CPS₍₂₎ and other policies, plans, agreements, contracts or procedures, where the subject of the dispute is between this CPS₍₂₎ and:

1. a service provider Operating Agreement, the Operating Agreement shall prevail;
2. a CPS₍₁₎, the CPS₍₁₎ shall prevail;
3. a subscriber agreement, this CPS₍₂₎ shall prevail;
4. any policy, plan, procedures or any other operational or practices documentation whatsoever, this CPS₍₂₎ shall prevail, excepting documents executed or authorised by SDPL that expressly change or exclude practices contained within this CPS₍₂₎ provided that a description of such changes or exclusions is appropriately published

2.4.3.2 Process

If a dispute arises in connection with these practices, the parties undertake in good faith to use all reasonable endeavours to settle the dispute by negotiation or mediation.

If the parties are not able to resolve a technical dispute within seven days from the date the dispute first arose, then the parties agree to jointly appoint an independent arbitrator, having appropriate qualifications and practical experience ("Arbitrator"), for the purpose of resolving the technical dispute and agree to be bound by the decision of that arbitrator. For the avoidance of doubt, a dispute over the Functionality Test or the Integration Test is an example of a technical dispute.

If the parties are not able to agree on an Arbitrator within 14 days from the date the dispute first arose, then the parties agree to appoint the person nominated by the President for the time being of the Australian Institute of Arbitrators. Either party may request the President of the Australian Institute of Arbitrators to make such a nomination.

The parties will promptly furnish to the Arbitrator (imposing appropriate obligations of confidence) all information reasonably requested by the Arbitrator relating to the dispute.

The Arbitrator will use all reasonable endeavours to render the Arbitrator's decision within 30 days following receipt of the information requested or if this is not possible, as soon as practical thereafter, and the parties must co-operate fully with the Arbitrator to achieve this objective.

The parties will share equally the fees and expenses of the Arbitrator.

2.5 Fees

2.5.1 Certificate issuance or renewal fees

Fees may be payable in respect to the issue or renewal of Certificates. Where fees are payable, the issuing CA must provide an up to date fee schedule to all its End Users, this may be done by publishing the fee schedule on a nominated web site.

2.5.2 Certificate access fees

Fees may be payable in respect to access to SDPL X.500 Directory services for Certificate downloading. Where fees are payable, SDPL provides an up to date fee schedule to all its End Users, this may be done by publishing the fee schedule on a nominated web site.

2.5.3 Revocation or status information access fees

Fees may be payable in respect to access to SDPL X.500 Directory services for Certificate revocation or status information. Where fees are payable, SDPL provides an up to date fee schedule to all its End Users, this may be done by publishing the fee schedule on a nominated web site.

2.5.4 Fees for other services such as policy information

No fee is to be levied for access to a CPS₍₁₎ or this CPS₍₂₎ via the Internet. A fee may be charged by an issuing CA for printed copies of a CPS₍₁₎ or this CPS₍₂₎. Printed copies of this CPS₍₂₎ are available from SDPL for a fee of \$AUD5.00 plus postage and packaging.

Fees may be payable in respect to the revocation or suspension of Certificates. Where fees are payable, the issuing CA must provide an up to date fee schedule to all its End Users, this may be done by publishing the fee schedule on a nominated web site.

2.5.5 Refund policy

SDPL or individual CAs under the SDPL RCA may establish a refund policy. Where a refund policy applies, an up to date refund policy is provided to all End Users, this may be done by publishing the refund policy on a nominated web site.

2.6 Publication and repository

2.6.1 Publication of CA information

This CPS₍₂₎ is published under the International Standard Book Number (ISBN) system.

2.6.1.1 Electronic Publication

This CPS₍₂₎ is published electronically in PDF format on the Security Domain and other nominated web sites at:

www.secdom.com.au

www.baltimore.com

The electronically published copy is hashed using the SDPL Root CA Hash. The resulting hash value is also published on the above web sites.

Users of this CPS₍₂₎ may hash this document using the Root CA public key, available from the SDPL X.500 Directory services, then compare the resulting value with the published value to assure themselves of the published document's integrity.

The PDF file is downloadable from the web site.

A CD-Writable Disk version of this CPS₍₂₎ is held by the National Library of Australia, in compliance with Australian ISBN Agency requirements.

2.6.1.2 Hard Copy Publication

Paper copies of this document are available from SDPL, for a fee. Requests should be directed to:

**General Manager - Certificates On-Line
Security Domain Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
2060 AUSTRALIA**

2.6.1.3 Publication by CAs

All relevant CAs within the SDPL PKI must:

1. publish this document on the web site(s) where they publish their CPS₍₁₎; or,

2. provide a link on their CPS₍₁₎ web site(s) to the Security Domain web site, with an appropriate explanation that the link may be used to access a copy of this document.

2.6.2 Frequency of publication

Certificates are published promptly following their generation and issue. CRL publication is in accordance with section 4.4.9 *CRL Issuance Frequency*. Newly approved versions of this CPS₍₂₎ and relevant CPS₍₁₎ are published promptly.

2.6.3 Access controls

There are no access controls on the reading of this CPS₍₂₎ or of relevant CPS₍₁₎ on the web sites nominated for publication.

Access to Certificate information (including CRLs) within the X.500 Directory is limited to a single name search enquiry.

Appropriate access controls are used to restrict to authorised personnel the ability to write to or modify these items.

2.6.4 Repositories

The Repository for the SDPL PKI is provided through the SDPL X.500 Directory. This directory contains Certificate information for all Certificates issued within the SDPL PKI.

The directory does not contain any information of a confidential nature.

The SDPL X.500 Directory is a high availability service that provides relying parties with Certificate information services. The directory provides the following repository services to authorised enquirers:

1. advice of Certificate status, including:
 - access to the SDPL CRL for revoked Certificates;
 - access to notices of suspension for suspended Certificates;
2. download facility for all service provider and End User Certificates.

The directory services provided to an enquirer may span:

1. a single policy domain; or,
2. nominated policy domains; or,
3. all policy and Certificate domains.

2.6.4.1 X.500 Directory Functions

The X.500 Directory performs the following functions:

1. allow a name search enquiry on master directories or copies thereof 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.
2. provide access to public keys via Certificate download;
 3. automatically check the CRL prior to a Certificate being downloaded and advise the requesting party if the Certificate has been revoked.

2.6.4.2 X.500 Directory Contact Details

The contact details for the X.500 Directory are published in each CPS₍₁₎ within the SDPL hierarchy.

2.6.4.3 X.500 Directory Availability

Standard availability for the X.500 Directory is during standard business hours, i.e. 9:00 a.m. – 5:00 p.m. Monday to Friday, Australian Eastern Standard Time (EST) or Australian Eastern Daylight Savings Time (EDST) as applicable.

A Premium service is available under a customer agreement that provides 7 days x 24 hours availability.

2.6.4.4 Restrictions on X.500 Directory access and services

Access to Certificate information is limited to a single name search enquiry that accesses the master directory or a copy thereof. The search enquiry allows an enquirer to determine within the span of the directory services provided:

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

The repository does not:

1. provide access to End Users in any manner other than that stated in this CPS₍₂₎;
2. provide any information or services to End Users other than that information and those services listed in this CPS₍₂₎;
3. alter any Certificate details or notices that it receives.

2.6.4.5 Repository publication

The SDPL Repository promptly publishes new Certificates and changes in Certificate status, including revocation, notices of suspension and expiry.

The X.500 Directory is published on the Security Domain and other nominated web sites at:

www.secdom.com.au

www.baltimore.com

Copies of the Directory may be published at such other locations as are required for the efficient operation of the SDPL PKI and as may be prescribed in various CPS₍₁₎. These copies may contain the whole of the Directory structure or parts thereof.

2.6.4.6 CRL publication

Client operated CAs may independently publish full CRLs applicable to their policy domain(s) and/or regular notifications of newly revoked Certificates, e.g. daily or weekly lists.

CRLs published in this manner:

1. may be in any form expedient to the purposes of the CA, for example in an X.500 Directory, on paper or as e-mail messages;
2. do not form part of the SDPL Repository. SDPL is not liable for the publication of CRLs published by customer operated CAs or any consequence of malfeasance, tort or contractual breach arising from the publication thereof.
3. will not preclude End Users from using the SDPL X.500 Directory.

2.7 Compliance Audit

2.7.1 Frequency of entity compliance audit

The RCA reserves the right to conduct a comprehensive compliance audit of the practices documented in this CPS₍₂₎:

1. within one year of the commencement of operations of a client operated CA or RA service, at the sole expense of the client provided such expense is not excessive;
2. at any other time that it deems warranted and at its own expense, provided a minimum of one month's notice is given.

2.7.1.1 CA and RA Certificate Renewal Compliance Audit

The RCA conducts general compliance audits of subordinate CAs whenever a CA Certificate is due for renewal, at the sole expense of the CA, provided such expense is not excessive.

A substantial level of non-compliance with any of the following may result in the RCA rejecting the CA's request for Certificate renewal:

1. RCA-CA Operating Agreement;
2. various CPS₍₁₎ under which Certificates are issued;

3. this CPS₍₂₎.

CAs conduct general compliance audits of subordinate RAs whenever an RA Certificate is due for renewal, at the sole expense of the RA being audited, provided such expense is not excessive.

A substantial level of non-compliance with any of the following may result in the CA rejecting the RA's request for Certificate renewal:

1. CA-RA Operating Agreement;
2. various CPS₍₁₎ under which Certificates are requested;
3. this CPS₍₂₎.

CAs provide a copy of all audit reports they complete to the RCA. The RCA may use such audit reports:

1. to determine the effectiveness of the audits conducted by an auditing CA;
2. to identify the need to conduct its own CPS₍₂₎ compliance audit of the audited RA;
3. for any other purpose that promotes the efficient and trustworthy operation of the PKI, for example to assist in identifying operational trends or systemic deviations.

2.7.2 Identity/qualifications of auditor

Any firm or person contracted to perform a security audit on a CA or LRA must have significant experience in the application of PKI and cryptographic technologies.

2.7.3 Auditor's relationship to audited party

Aside from the audit function, the auditor and audited party shall not have any current or planned financial, legal, or other relationship that could result in a conflict of interest.

2.7.4 Topics covered by audit

The topics covered by a compliance audit will include but not be limited to:

1. Security Policy and Planning;
2. Physical Security;
3. Technology Evaluation;
4. CA Services Administration;
5. Personnel Vetting;
6. Relevant CPS₍₁₎ and CPS₍₂₎;

7. Contracts;
8. Privacy Considerations.

2.7.5 Actions taken as a result of deficiency

Internal and external audit reports are submitted to General Manager - Certificates On-Line.

When irregularities are found, General Manager - Certificates On-Line promptly implements appropriate corrections.

2.7.6 Communication of results

Audit results are considered to be sensitive commercial information. Unless otherwise specified in contract, they will be protected in accordance with section 2.8.

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

2.8.1.1 Collection and Use of Personal Information

Application of OECD Guidelines

The practices described in this CPS₍₂₎ conform to the OECD Guidelines on the use of public key infrastructure.

Application Privacy Legislation

Information supplied to SDPL service providers as a result of the practices described in this CPS₍₂₎ may be covered by national government or other privacy legislation or guidelines.

Confidential information

Access to confidential information by operational staff is on a need-to-know basis.

Paper-based records and other documentation containing confidential information are kept in secure and locked containers or filing systems, separate from all other records.

2.8.1.2 Registration information

All registration records are considered to be confidential information, including:

1. Certificate applications, whether approved or rejected;
2. POI documentation and details;
3. Certificate information collected as part of the registration records, but this does not act to prevent publication of Certificate information in the X.500

Directory;

4. subscriber agreements;
5. any information requested by SDPL when it receives an application from a third party to operate a CA within the SDPL chain of trust.

2.8.1.3 Certificate information

The reason for a Certificate being suspended or revoked is considered to be confidential information, with the sole exception of the revocation of a service provider's Certificate due to:

1. the compromise of their Private Key, in which case a disclosure may be made that the Private Key has been compromised;
2. the termination of the service provider, in which case prior disclosure of the termination may be given.

2.8.1.4 Service provider documentation

The following service provider documents are considered to be confidential:

1. Concept of Operations;
2. CA or RA Operating Agreement;
3. Protective Security Risk Review;
4. System Security Plan;
5. Contingency & Disaster Recovery Plan;
6. Configuration Baseline;
7. Operating Procedures.

2.8.2 Types of information not considered confidential

2.8.2.1 Certificate information

Certificate information published in the X.509 Directory is not confidential and is considered to be public knowledge, including:

1. Certificate status;
2. the date and time of Certificate suspension or revocation;
3. the period for which Certificate suspension applies.

2.8.2.2 Service provider documentation

The following service provider documents are public documents and are not considered to be confidential information:

1. CPS₍₁₎;
2. this CPS₍₂₎;
3. Security Policy (Public);
4. Privacy Policy (Public);
5. Certificate Key Management Plan (Public).

2.8.3 Disclosure of Certificate revocation/suspension information

2.8.3.1 Disclosure of Certificate suspension information

Information on Certificate suspension is not disclosed. The Directory provides information indicating the fact of suspension, but not the reason for the suspension status.

2.8.3.2 Disclosure of Certificate revocation information

Certificate revocation information is provided via the CRL in the SDPL X.500 Directory services.

2.8.4 Release to law enforcement officials

As a general principle, no document or record belonging to Security Domain is released to law enforcement agencies or officials except where:

1. a properly constituted warrant is produced; and
2. the law enforcement official is properly identified.

Registration Records are only releasable to law enforcement agencies and officials of those agencies where:

1. a properly constituted warrant is produced; and,
2. the law enforcement official is properly identified.

2.8.5 Release as part of civil discovery

As a general principal, no document or record belonging to Security Domain is released to any person except where:

1. a properly constituted instrument requiring production of the information is produced; and,
2. the person requiring production is a person authorised to do so and is properly identified.

2.8.6 Disclosure upon owner's request

The subject of a Registration Record has full access to that record, and is empowered to authorise release of that record to another person.

Formal authorisation may take two forms:

1. a properly constituted electronic request providing that the request is digitally signed by a valid digital signature under a recognised CPS₍₁₎; or,
2. by application in writing.

No release of information is permitted without a formal authorisation.

2.8.7 Other information release circumstances

No other release of information is permitted without a formal authorisation.

2.9 Intellectual Property rights

2.9.1 General provision

Security Domain Pty Limited warrants that it is in possession of, or holds licences for the use of hardware and software in support of this CPS₍₂₎.

Security Domain Pty Limited further warrants that operational use of this CPS₍₂₎ does not infringe any copyright enforceable in Australia of any third party. The use of the PKIX IETF Draft 4 Guideline is acknowledged.

Security Domain Pty Limited excludes all liability for breach of any other intellectual property rights.

2.9.1.1 SDPL PKI

All Intellectual Property Rights including all copyright in all certificates and all documents (electronic or otherwise) belongs to and will remain the property of the CA.

2.9.1.2 Public and private keys

If the end user generates the public and private key pair to the satisfaction of the CA then the end user grants to the CA the right to publish and propagate in the CA Directory the public key that corresponds to the private key that is in the possession of the end user. This publication will be through the incorporation of the public key in the certificate (whether electronic or otherwise) that forms part of the CA Directory. Nothing in this clause grants to the end user any rights whatsoever in relation to the format or structure of the certificate that encompasses the end users public key.

If the RA generates the end users public and private key pair then the RA assigns to the end user all intellectual property including copyright (if any) in the private key but not the public key. The RA grants to the CA the right to publish and propagate in the CA Directory the public key that corresponds to the private key that is in the possession of the end user. This publication will be through the incorporation of the public key in the certificate (whether electronic or otherwise) that forms part of the CA Directory. Nothing in this clause grants to the RA or the end user any rights whatsoever in relation to the format or structure of the certificate that encompasses the end users public key .

2.9.1.3 Certificate

The CA reserves the right at any time to cancel or suspend any certificate in accordance with the procedures and policies set out in this policy statement.

2.9.1.4 Distinguished names

Intellectual property rights in distinguished names vest in the assigning RA unless otherwise specified in a CPS₍₁₎, contract or other agreement, e.g. subscriber agreement.

2.9.2 Copyright**2.9.2.1 General**

The intellectual property in this CPS₍₂₎ is the exclusive property of Security Domain Pty Limited.

2.9.2.2 in OID

Copyright in the Object Identifiers (OID) for the SDPL PKI vest solely in Security Domain Pty Limited.

OIDs are not to be copied, used or otherwise dealt with in any way except as provided for in the operation of the SDPL infrastructure, or in accordance with the relevant CPS₍₁₎ or this CPS₍₂₎.

3. IDENTIFICATION AND AUTHENTICATION

3.0 General

3.0.1 CA and RA initial registration

A fundamental concept underpinning the operation of SDPL's PKI is trust. Trust must be realised in each and every aspect of the service operation. At SDPL's discretion, other trustworthy parties may be permitted to operate CA and RA services within SDPL's chain of trust.

To ensure the integrity and trustworthiness of operations throughout the PKI hierarchy, client operated CAs and RAs must agree during registration to comply with the practices in this CPS⁽²⁾.

3.0.1.1 Submission of application to operate a CA or RA

An application by a third party to establish and operate a CA and/or RA within the SDPL chain of trust should be made in the form of a letter of request (on organisational letterhead) to:

**General Manager – Certificates On-Line
Security Domain Pty Ltd
Level 5, 1 James Place
NORTH SYDNEY NSW
2060 AUSTRALIA**

SDPL does not permit private individuals to operate as CA or RA services.

Applications to operate a CA or RA service must include the following details, which may be appended to the letter of request:

1. the legal name of the party making the application;
2. any registered business names or other trading names used by the applicant relevant to the operation of the proposed CA or RA service;
3. the proposed name under which the CA or RA will be operating;
4. the domain name and IP address for CA or RA operations;
5. full contact details as follows:
 - residential and mailing address;
 - telephone and facsimile number(s);

- e-mail address;
 - authorised representatives and their contact details;
 - designated operational/administrative contacts and their contact details;
6. a statement that the applicant:
- has read this CPS₍₂₎;
 - agrees to contractually bind the proposed CA or RA service to the practices prescribed therein.

3.0.1.2 Consideration of Application

When SDPL receives an application from a third party to operate a CA and/or RA within the SDPL chain of trust:

1. an authorised representative of the applicant attends a registration interview in person. During the interview, the representative produces original copies of POI documentation totalling a minimum of 100 points;
2. the applicant:
 - submits a Concept of Operations (CONOPS) document for SDPL's approval;
 - enters into a contractual relationship by signing an RCA-CA Operating Agreement and/or a CA-RA Operating Agreement;
 - submits the CPS₍₁₎ under which Certificates will be issued to the SDPL PAA for approval;
3. SDPL approves or rejects the application. SDPL is under no obligation to disclose its reasons, or information considered, in rejecting an application. SDPL reserves the right to revoke its approval if subsequent requirements for the commencement of operations are not met in full or to its satisfaction.

3.0.1.3 Requirements for commencement of operations

If the application to operate CA or RA services is approved, prior to commencement of operations:

1. SDPL advises the new service of its OID and distinguished name;
2. the SDPL RCA provides:
 - CA or RA software and hardware;
3. the new CA or RA establishes under SDPL's auspices, a range of policy, planning and operational documentation including:
 - Protective Security Risk Review;
 - System Security Plan;

- CA or RA Operating Procedures.
- 4. the new CA or RA generates its own keys, then has its public keys certified by the SDPL RCA;
- 5. all operational procedures are vetted for compliance before they are implemented.

3.0.2 End user initial registration

3.0.2.1 Pre-registration interview

End Users making their initial application for a Certificate under a relevant CPS₍₁₎ are to be provided with the following information, during a pre-registration interview that may be completed immediately prior to registration:

1. an explanation of the nature, purpose and effect of the relevant CPS₍₁₎ and this CPS₍₂₎;
2. copies of relevant CPS₍₁₎ and this CPS₍₂₎, or the web site addresses where they are published;
3. their rights, obligations and duties under the relevant subscriber agreement;
4. advice of the documentation required for POI purposes;
5. if applicable, the End User's right to generate their own keys;
6. End Users may additionally be informed of various Certificate types that may be available to them.

The above information may alternatively be provided to End Users in written form a reasonable time before the registration interview, together with contact information for any questions the End User may have.

3.0.2.2 Registration interview

The practices described in this section apply to all End Users making:

1. their initial application for a Certificate under a relevant CPS₍₁₎;
2. any subsequent application for a new Certificate under that CPS₍₁₎.

This section does not apply to Certificate renewal, unless otherwise provided for within this CPS₍₂₎ or the pertinent CPS₍₁₎.

The registration interview is to:

1. be attended by the End User in person, in the case of an organisation the registration is to be attended by an authorised representative;
2. be conducted by an authorised registrar;
3. perform the following functions:

- collection of Certificate information;
- POI;
- proof of other material Certificate information;
- completion of a subscriber agreement;
- acceptance of public keys generated by the End User (if applicable).

Where the RA generates key pairs for the End User, this may be done during the registration interview, or as post-interview processing of the Certificate application.

The End User's distinguished name, which is decided by the registrar, may also be confirmed during the interview or determined during post-interview processing.

At the end of the interview, the End User is provided with a copy of all forms and other documentation completed, including a copy of the Certificate information, the POI form, the subscriber agreement and any notes made by the registrar.

Collection of Certificate information

The information required for the issuing of the requested Certificate is obtained from the End User. The End User's contact details are additionally obtained at this time. The full information collected typically includes:

1. Certificate type;
2. full name (for individuals);
3. organisation and department (for organisational End Users);
4. e-mail address;
5. other contact details such as telephone number, facsimile number and mailing address;
6. other information may be required specific to the individual RA's operations and/or the nature of the Certificate usage, for example:
 - billing information such as an organisational cost centre number;
 - attributes that are to be included in an Attribute Certificate;
 - an access control mechanism to identify the user in the event of a telephone request for Certificate revocation.

This information may be collected on a paper-based form (e.g. a Certificate application form) for later processing or entered directly into the RA software.

Registrars are to make reasonable efforts to confirm the accuracy of Certificate information. Individual CPS₍₁₎ may prescribe specific criteria for the authentication of information critical to Certificate usage, for example:

1. in the event that an End User's residential address is considered by a community of interest to be material Certificate information, and is included in Certificates issued under a relevant CPS₍₁₎, Registrars may be required to follow a set procedure to verify that address;
2. specific documentation may need to be sighted to verify an organisation's:
 - membership in a chamber of commerce or industry body;
 - compliance with certain standards, for example ISO9000.

Proof of Identity

The POI documentation offered by the End User must be original copies that have been issued without alteration or erasure.

The registrar is to:

1. record the POI documentation they sight on a POI form that complies with the recommended form published in the CPS₍₁₎;
2. in the presence of the End User:
 - take a copy of each document and seal those copies in an envelope;
 - attach the POI form to the front of the envelope.

Specific criteria for POI are contained in relevant CPS₍₁₎.

Proof of employment

Where a Certificate verifies a person's employment, or Certificate use is based upon the person's authority as a result of their employment, proof of employment must be obtained during initial registration. Specific criteria for proof of employment are contained in relevant CPS₍₁₎.

Proof of employment is typically accomplished by the applicant furnishing a request on organisational letterhead:

1. for the issue of a nominated type of Certificate;
2. signed by an authorised officer whose signature is known to the registrar.

Completion of a subscriber agreement

The subscriber agreement is to comply with the recommended agreement published in the CPS₍₁₎.

Prior to obtaining the End User's signature on the agreement, the registrar is to confirm that the End User understands their rights, obligations and duties under the agreement as explained during the pre-registration interview. The End User may take a copy of the subscriber agreement and other relevant documentation to seek advice from a solicitor, etc. prior to signing.

The subscriber agreement must be signed in the presence of the registrar.

Acceptance of public keys generated by the End User

In the event that key pairs have been generated by the End User, the registrar is to ensure during post-interview processing that the applicant is:

1. in possession of the associated private keys, this may typically be accomplished by exchanging digitally signed and encrypted e-mail messages with the applicant; and,
2. the true owner of the key pairs, this may typically be accomplished by:
 - the RA checking, and arranging for any other RAs within the policy domain to check, its records to ensure the public keys are not already listed against any current operational or revoked Certificate;
 - additionally, if deemed appropriate, obtaining a statutory declaration to that effect.

The registrar is to additionally determine during post-interview processing that the public keys are of the required key length.

3.0.2.3 Post-Registration interview processing

After the registration interview has been completed, the registrar considers the Certificate application and approves or rejects it.

If the application is approved, the registrar uses the RA software to transmit a digitally signed Certificate request to the issuing CA.

If the application is rejected, the applicant is to be promptly informed. The registrar and the RA are under no obligation to disclose the reason for the rejection of any Certificate application, except where required by the CPS₍₁₎ under which the Certificate was to have been issued, or by law or government regulation. A person or organisation whose application has been rejected may reapply not less than three months after the date of the application.

3.1 Initial registration

3.1.1 Types of names

All Certificate holders require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

The SDPL RCA approves naming conventions for the creation of distinguished names for Certificate applicants. Different naming conventions may be used in different policy domains.

RAs propose and approve distinguished names for Certificate applicants, and as a minimum check that a proposed distinguished name is unique, verify that the name is not already listed in the SDPL X.500 Directory.

3.1.2 Need for names to be meaningful

Distinguished names must be meaningful. Pseudonymous names may be used in the common name component of a distinguished name where requested by an End

User, provided the End User can satisfactorily establish their right to use the pseudonym.

RAs are not to accept pseudonymous names which they believe may cause offence.

The SDPL PKI supports the use of certificates as a form of identification within a particular community of interest. Anonymous certificates are not supported by the SDPL PKI.

3.1.3 Rules for interpreting various name forms

The normal operation of some types of Certificate generation requires the insertion of an organisation name and department as part of the distinguished name.

Where a CPS₍₁₎ does not require an organisation identifier or department identifier in a Certificate, the following changes are to be made to the distinguished name:

Organisation name	Not Applicable
Department name	Not Applicable

3.1.4 Uniqueness of names

Distinguished names are to be unambiguous and unique.

3.1.5 Name claim dispute resolution procedure

Any dispute regarding a Distinguished Name is resolved in terms of section 2.4.3.3 *Process*.

3.1.6 Recognition, authentication and role of trademarks

This is a commercial issue and as such is defined by relevant contractual documents.

3.1.7 Method to prove possession of private key

Where key pairs are generated by an End User, the registrar must satisfy themselves that the End User does in fact possess the private keys that correspond to the public keys received from the End User.

This may typically be accomplished by exchanging digitally signed and encrypted e-mail messages with the applicant.

The registrar is to also take reasonable steps to ensure the End User is the true owner of the key pairs. Reasonable steps might typically consist of:

1. the RA checking, and arranging for any other RAs within the policy domain to check, its records to ensure the public keys are not already listed against any current operational or revoked Certificate; and,
2. additionally, if deemed appropriate, obtaining a statutory declaration from the End User that they are the true owner of the key pairs.

If any doubt exists, the registrar is not to request certification. If the End User's right to use or possession of self-generated keys cannot be shown or proven, or reasonable doubt exists:

1. the applicant's details are to be reported to the CA;
2. the application may be progressed using key pairs generated by the RA.

3.1.8 Authentication of organization identity

An organisation's identity is to be authenticated:

1. during an interview with an authorised registrar attended in person by an authorised representative of the organisation;
2. in compliance with:
 - the POI practices described in this CPS₍₂₎;
 - the process and forms described in the relevant CPS₍₁₎.

No on line techniques are approved for organisational identification.

3.1.9 Authentication of individual identity

An individual's identity is to be authenticated:

1. during an interview with an authorised registrar attended in person by the individual;
2. in compliance with:
 - the POI practices described in this CPS₍₂₎;
 - the process and forms described in the relevant CPS₍₁₎.

No on line techniques are approved for individual identification.

3.2 Routine Rekey

End Users may request Certificate renewal provided that:

1. the request is made prior to the expiry of their current Certificates;
2. material Certificate information as contained in registration records has not changed;
3. their current Certificates have not been revoked;
4. their keys are not listed as compromised keys;
5. they are not listed as a compromised user.

If any of these conditions are not met, the End User must apply for a new Certificate, providing all information and documentation required at an initial registration interview and signing a new subscriber agreement.

Certificate renewal is governed by the associated CPS₍₁₎. Where a CPS₍₁₎ provides for on line renewal requests, such requests must be digitally signed by the End User. A CPS₍₁₎ may require on line requests to comply with a prescribed file format, or may allow End Users to send free-form e-mail messages, etc.

In the event that on line requests are not provided for in a CPS₍₁₎ or are not possible for particular End Users, End Users must attend a Certificate renewal interview in person with an authorised registrar, during which they may be required to produce identification and/or other authentication documentation in compliance with the CPS₍₁₎. The End User must make a renewal request in writing that is signed in the presence of the registrar, who is to verify the End User's signature.

Key pairs must always expire at the same time as the associated Certificate. When an End User requests Certificate renewal, they are requesting both new Certificates and new key pairs.

CAs are to verify and process Certificate renewal requests on the day they are received.

3.3 Rekey after Revocation

Rekey is not permitted after Certificate revocation. End Users requiring a replacement Certificate after revocation must:

1. attend an initial registration interview; and,
2. apply for a new Certificate, complying with all initial registration interview procedures and requirements as though they were a new user.

3.4 Revocation request

A request to revoke keys and Certificates, if initiated by an authorised party and signed by a valid key and Certificate under the relevant CPS₍₁₎ constitutes a valid and enforceable revocation request.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

It is the responsibility of individuals, organisations and government departments, agencies and authorities requiring keys and Certificates to make that request to an approved RA.

Certificate applicants must choose the type of Certificate they require. Registrars may advise applicants on the functionality, authority levels, security services and other attributes or characteristics of differing Certificate types and may recommend the Certificate type that best suits the applicant's needs. However, the decision to apply for a Certificate is to be made solely by the applicant, and the applicant is to independently assess and determine the appropriateness of any type of Certificate for a specific purpose.

There may be many RAs issuing Certificates for a particular policy domain. These RAs may be differentiated by their geographical proximity to the Certificate applicant, the type of Certificates they are authorised to issue or by their organisational relationship to the Certificate applicant's department.

4.2 Certificate issuance

RAs and CAs are to take reasonable care in accepting and processing Certificate applications. They are to comply with the practices described in this CPS₍₂₎ and with any requirements imposed by the CPS₍₁₎ under which the Certificate is being issued.

In particular, care should be taken to ensure Certificate information does not contain any factual misrepresentations and that no data entry errors are made when accepting an application or generating a Certificate.

RAs and CAs are not responsible for monitoring, investigating or confirming the accuracy of Certificate information after a Certificate has been issued. Where advice is received that Certificate information is inaccurate or no longer applicable, the Certificate may be revoked and a new Certificate applied for.

4.2.1 Certificate issue process

The Certificate issue process is governed by the CPS₍₁₎ under which the Certificate is issued. Typically, Certificate issue involves:

1. the End User personally attending a registration interview, during which an authorised registrar:
 - obtains the End User's registration details and Certificate information;
 - authenticates critical Certificate information such as the user's identity;
 - explains the appropriate CPS₍₁₎ and this CPS₍₂₎ to the user, and the user's

- responsibilities attached to possession and use of their public keys and Certificates;
- obtains in their presence, the End User's signature on a subscriber agreement;
2. the RA generates the Certificate key pairs and provides the End User with an associated Personal Identification Code (PIC). The PIC is required to access the keys and Certificates when they are later delivered to the End User via a secure transport medium. Note that:
- some CPS₍₁₎ may allow key pairs to be generated by the End User as well as by the RA in which case, the End User must prove possession of the private keys corresponding to the public keys supplied to the RA, and must establish their right to use the key pairs;
 - the practice of using a PIC is recommended but not mandatory. In certain situations, for example the transport of keys and Certificates in a physically secure environment between trusted parties, a CPS₍₁₎ may exclude the use of a PIC;
 - some CPS₍₁₎ may require the PIC to be split into two portions that are delivered to the End User by different methods, to mitigate against the risk of the PIC being intercepted by a third party;
3. the registrar processes the End User's Certificate application and submits a Certificate request to the issuing CA for each public key, together with the public keys;
4. the issuing CA receives the Certificate requests and keys. On the day of receipt the CA verifies each request, generates and signs the requested Certificates, then:
- posts the Certificates to the SDPL X.500 Directory;
 - issues the Certificates to the RA;
5. the RA sends the End User an e-mail message, or advises them by other means, that their keys and Certificates are available. Some CPS₍₁₎ may require the keys and the Certificates to be attached in a secure format to the e-mail message;
6. the End User:
- installs a recognised End User application on their PC;
 - accesses their keys and Certificates in a secure format. The keys and Certificates may be retrieved from a web site, attached to an e-mail message, delivered via removable storage media or accessible on a network drive;
 - uses their PIC to import the keys and Certificates into their End User application. During the import process, the End User protects the private keys being stored on their PC by entering an access control mechanism known only to them;
7. the End User's keys and Certificates are now ready for operational use.

Relying parties

Relying parties need to access nominated Certificates for the authentication of digital signatures and/or decryption of secured files. They may obtain the Certificates they require directly from Certificate owners, or by requesting Certificates from the SDPL X.500 Directory services.

4.2.1.1 End User's consent required

Certificates should not be issued:

1. without an End User's consent;
2. through an RA other than where the Certificate application was made.

For the purposes of this CPS₍₂₎, a signed subscriber agreement is deemed to be the End User's specific consent to, and request for the issue of Certificates through the registering RA.

4.2.1.2 CAs' right to reject Certificate requests

Certificates are issued at the discretion of the CA receiving a Certificate request. All CAs have the right to reject a Certificate request. If a Certificate request is rejected, the requesting RA is to promptly inform the applicant. CAs are under no obligation to disclose the reason for the rejection of any Certificate request, except where required by the CPS₍₁₎ under which the Certificate was to have been issued, or by law or government regulation. A person or organisation whose Certificate request has been rejected may reapply not less than three months after the date of the Certificate application.

4.2.1.3 Operational periods

All Certificates begin their operational period on the date of issue. The operational period of a Certificate is governed by:

1. the RCA-CA agreement;
2. the CA-RA agreement;
3. the CPS₍₁₎.

The expiry date of issued Certificates must not result in an operational period greater than that permitted by the above instruments. In the event that a Certificate is issued with a greater than permitted operational period, the Certificate is to be revoked.

4.3 Certificate Acceptance

An End User's receipt of a Certificate, and their subsequent use of their keys and Certificates, constitutes Certificate acceptance.

By accepting a Certificate, the user:

1. agrees to be bound by the continuing responsibilities, obligations and duties imposed on them by their subscriber agreement, the associated CPS₍₁₎ and this CPS₍₂₎;

2. warrants that to their knowledge no unauthorised person has had access to the private key associated with the Certificate;
3. asserts that the Certificate information they have supplied during their registration interview is truthful and has been accurately and fully published within the Certificate.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

Revocation can be described as no longer being able to use a Certificate. A service provider or End Users' Certificate is revoked when:

1. the Certificate owner or their keys or Certificates are compromised through:
 - the theft, loss, disclosure, modification, or other compromise or suspected compromise of the user's private key(s);
 - the deliberate misuse of keys and Certificates, or a substantial non-observance of operational requirements in the subscriber agreement or associated CPS₍₁₎ or of the practices in this CPS₍₂₎;
2. a Certificate owner leaves the SDPL community of interest, for example:
 - an organisational End User leaves the employment of their organisation;
 - a service provider ceases operations;
 - the decease of an End User;
3. there is an improper or faulty issue of a Certificate due to:
 - a material prerequisite to the issue of the Certificate not being satisfied;
 - a material fact in the Certificate is known or reasonably believed to be false;
 - data entry or other processing errors;
4. an End User generates the keys associated with a Certificate and those keys are found to be weak;
5. material Certificate information becomes inaccurate, for example when the owner of:
 - an identity Certificate changes their name;
 - an attribute Certificate obtains increased system privileges;
6. a properly formatted request is received from an End User;
7. a validated request is received from an authorised third party, for example:

- a court order;
 - a request made by a person with power of attorney;
8. the Certificate of a superior RA or CA is revoked;
 9. it is known or there is reason to believe a service provider does not possess the financial resources to maintain its Certificate services.

4.4.2 Who can request revocation

Certificate revocation can be initiated by:

1. any service provider who is in the Certificate owner's chain of trust and is in a superior position in that chain;
2. the owner of the Certificate;
3. an authorised third party.

End Users may request revocation of their Certificates for any reason, or for no reason, and must request revocation under the conditions specified in 4.4.1 - *Circumstances for revocation*.

Service providers may not request the revocation of, or revoke their own Certificates under any conditions other than those described in 4.4.1 - *Circumstances for revocation*.

4.4.2.1 CAs

CAs operating within the SDPL hierarchy must initiate revocation under the conditions described in 4.4.1 - *Circumstances for revocation*.

4.4.2.2 RAs

RAs operating within the SDPL hierarchy must initiate revocation under the conditions described in 4.4.1 - *Circumstances for revocation*.

4.4.2.3 End Users

End Users may request the revocation of their own Certificates for any reason, and must make such requests through an authorised RA.

4.4.2.4 Authorised third parties

Authorised third parties may request Certificate revocation through an authorised RA. Such authorised parties include, but are not limited to:

1. authorised officers in an organisational End User's organisation, requesting revocation when the End User leaves the employment of the organisation, in which case the RA must verify the officer's authorisation and that the request has actually been initiated by that officer;
2. third parties with Power of Attorney, in which case the RA must verify the Power of Attorney and the identity of the relevant person;

3. the executor of a Certificate Owner's estate, in which case the RA must verify the Certificate Owner's decease, and the appointment and identity of the executor;
4. a Court with jurisdiction within the issuing CA's area of operations, in which case the RA must confirm the validity of the court order.

Note that a court order for Certificate revocation may be served directly on an issuing CA.

4.4.3 Procedure for revocation request

The practices involved in processing of a revocation request will vary depending on the identity of the originator. This section describes the practices where revocation is:

1. requested by the End User;
2. verified by an RA;
3. processed by a CA.

Where a revocation request is originated by a party other than the End User:

1. the practices employed in processing the request will comply to the fullest extent possible with the practices that are described below;
2. the reason for the request must be documented.

4.4.3.1 CA processing

To process a revocation request initiated by an RA, a CA:

1. receives and authenticates the digitally signed request from the RA;
2. prioritises the request according to the revocation response times contained within the relevant CPS₍₁₎;
3. revokes the Certificate;
4. adds the Certificate to its CRL in the X.500 Directory;
5. issues a notice containing the Certificate details and the date and time of revocation to the Certificate owner and for organisational users, to the user's organisation. The notice is not to include the reason for revocation.

Note that:

1. revoked Certificates are not deleted from a CA's directory services;
2. CAs may employ additional methods to issue notices of revoked Certificates to their users.

4.4.3.2 RA processing

To process a revocation request initiated by an End User, an RA:

1. receives and authenticates the request;
2. ensures the Certificate and public key are current;
3. prioritises the request according to the processing times indicated in the relevant CPS₍₁₎;
4. if applicable:
 - adds the user's keys to its list of compromised keys;
 - adds the user to its list of compromised users;
5. sends a digitally signed revocation request to the CA.

The RA verification requirements for revocation requests are the same as for Certificate renewal, and because of these requirements such requests must be delivered to the RA either in the form of digitally signed file, or in person. If delivered in person, the request must be signed in the presence of the registrar.

4.4.3.3 Certificate Revocation Request

A Certificate revocation request, whether in paper or electronic (e.g. e-mail) form, is to contain the information illustrated in the example form below.

Certificate Revocation Request	Date : _____
To: <RA NAME> <RA ADDRESS>	
Section 1 - Certificate details (if known)	
Certificate ID:
Certificate serial number:
Certificate type:
Section 2 - Certificate owner details	
Full Name: (For private individuals, show family name last.)
Organisational users only:	
Organisation:
Department:
Section 3 - Reason for revocation *	

<p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>	
<p>* This section is optional for Certificate owners requesting revocation of their own Certificates.</p>	
<p>Section 4 – Authorisation</p>	
<p>Authorised by:</p>	<p><input type="checkbox"/> Certificate owner</p> <p><input type="checkbox"/> Authorised third party (Original documentation verifying authorisation must be sighted.)</p>
<p>Signature:</p>	<p>.....</p>

4.4.3.4 Certificate owner duties

The owner of a revoked Certificate is to:

1. continue to safeguard the private key associated with the revoked Certificate, until the date of Certificate expiry; or,
2. securely destroy the private key associated with the revoked Certificate.

4.4.4 Revocation request grace period

Revocation requests are to be:

1. verified on receipt;
2. actioned as appropriate within the processing times stipulated within the relevant CPS⁽¹⁾.

4.4.5 Circumstances for suspension

Certificate suspension is not supported.

4.4.6 Who can request suspension

Certificate suspension is not supported.

4.4.7 Procedure for suspension request

Certificate suspension is not supported.

4.4.8 Limits on suspension period

Certificate suspension is not supported.

4.4.9 CRL issuance frequency

The CRL in the X.500 Directory is updated at the time of Certificate revocation.

4.4.10 CRL checking requirements

Relying parties should regularly check the validity and currency of a Certificate.

SDPL recommends that relying parties should check at least weekly, however where the value, importance or sensitivity of a message, transaction or other file is high, it is recommended that the relying party checks on a per transaction basis.

4.4.11 On-Line revocation/status checking availability

SDPL provides an on line X.500 Directory for verifying the status of Certificates issued within the SDPL PKI.

4.4.12 On Line revocation checking requirements

Refer to section 4.4.10 - *CRL checking requirements*.

4.4.13 Other forms of revocation advertisements available

Some CPS₍₁₎ may support other forms of revocation advertisement, such as a locally distributed CRL.

SDPL operated CAs use only the X.500 Directory for CRLs.

4.4.14 Checking requirements for other forms of revocation advertisements

Where other forms of revocation advertisement are supported, checking requirements are specified in the relevant CPS₍₁₎.

4.4.15 Special requirements re key compromise

There are no variations to the above Certificate revocation and suspension procedures when the revocation or suspension is due to private key compromise.

4.5 Security Audit procedures

The SDPL RCA, SDPL CA and SDPL RA maintain, and all approved CAs and RAs are obliged under contract to maintain, adequate records and archives of information pertaining to the operation of the public key infrastructure.

RCA, CA and RA software automatically preserves an audit trail for the three primary states in the CMLC, i.e. generation, operational use and expiry.

4.5.1 Types of event recorded

The minimum audit records to be kept include all:

1. types of registration records, including records relating to rejected applications;
2. key generation requests, whether or not key generation was successful;
3. Certificate generation requests, whether or not Certificate generation was successful;
4. Certificate issuance records, including CRLs;
5. audit records, including security related events.

4.5.2 Frequency of processing log

Audit logs are processed on a daily, weekly, monthly and annual basis.

4.5.3 Retention period for audit log

Audit logs are retained for a minimum of seven years. They are maintained 'on site' for a minimum period of three months and a maximum period of twelve months.

4.5.4 Protection of audit log

Audit logs are encrypted using a key and Certificate specifically generated for the purpose.

4.5.5 Audit log backup procedures

Each service provider in the SDPL hierarchy is to establish and maintain a backup procedure for audit logs.

4.5.6 Audit collection system

The SDPL PKI audit collection system is a combination of automated and manual processes performed by the CA or RA operating system, the CA or RA application, and by operational personnel.

Type of event	Collection System	Recorded by
Successful and failed attempts to changes operating system security parameters.	Automatic	Operating system
Application startup and shutdown.	Automatic	Operating system
Successful and failed log-in and log-off attempts.	Automatic	Operating system
Successful and failed attempts to create, modify, or delete system accounts.	Automatic	Operating system
Successful and failed attempts to create, modify or delete authorised system users.	Automatic	Operating system
Successful and failed attempts to request, generate, sign, issue or revoke keys and Certificates.	Automatic	CA or RA software

Type of event	Collection System	Recorded by
Successful and failed attempts to create, modify or delete Certificate holder information.	Automatic	RA software
Backup, archiving and restoration.	Automatic and manual	Operating system and operations personnel
System configuration changes.	Manual	Operations personnel
Software and hardware updates.	Manual	Operations personnel
System maintenance.	Manual	Operations personnel
Personnel changes	Manual	Operations personnel

4.5.7 Notification to event-causing subject

Operations personnel notify their security administrator when a process or action causes a critical security event or discrepancy.

4.5.8 Vulnerability assessments

A Protective Security Risk Review (PSRR) has been completed for the entire SDPL hierarchy. This PSRR covers the overarching risks and threats that may impact the public key infrastructure.

Individual threat and risk assessments are required at each subordinate entity level e.g. approved CA and RAs.

4.6 Records Archival

Each service providers in the SDPL hierarchy maintains an archive of relevant records described in this policy.

4.6.1 Types of event recorded

The following audit information is recorded and archived by service providers:

1. audit logs;
2. Certificate request information;
3. Certificates, including CRLs generated;
4. Complete back up records;
5. copies of e-mail logs;
6. formal correspondence.

4.6.2 Retention period for archive

4.6.2.1 Secure maintenance of keys

In accordance with OECD Guidelines only confidentiality keys are archived. The minimum period for archiving confidentiality keys is seven years from the date of expiry of the Certificate associated with the key, unless another period is specified in the relevant CPS₍₁₎.

Confidentiality keys are archived securely on a CD ROM.

4.6.2.2 Secure maintenance of Certificate

Certificates are archived for a minimum period of seven years from the date of expiry, unless another period is specified in the relevant CPS₍₁₎.

Certificates are archived securely on a CD ROM.

4.6.2.3 Term of archive maintenance

Audit trail information is kept for a minimum period of seven years from the date of generation, unless another period is specifically required.

Audit logs are archived securely on a CD ROM.

4.6.3 Protection of archive

Archive media is protected either by physical security, or a combination of physical security and cryptographic protection. It is also protected from environmental factors such as temperature, humidity, and magnetism.

4.6.4 Archive backup procedures

Each service provider has established archive back up procedures to ensure and enable complete restoration of current service in the event of a disaster situation.

4.6.5 Requirements for time-stamping of records

Trusted third party time stamping is not supported.

4.6.6 Archive collection system

Each service provider is to establish an archive collection system that meets the requirements of this CPS₍₂₎.

4.6.7 Procedures to obtain and verify archive information

The integrity of a service provider's archives are verified:

1. at the time the archive is prepared;
2. annually at the time of a programmed Security Audit;
3. at any other time when a full security audit is required.

4.7 Key changeover

Key changeover is not automatic. Keys expire at the same time as their associated Certificates and, with the exception of the RCA which issues a new Certificate and new keys to itself, all parties within the SDPL PKI are to obtain new keys by making an application for Certificate renewal a minimum of two weeks prior to Certificate expiry.

Service providers must:

1. ensure that key changeover causes minimal disruption to subordinate service providers and End Users in their chain of trust;
2. provide End Users and any subordinate CAs or RAs with a minimum of three months' notice of planned key changeover.

4.8 Compromise and Disaster Recovery

Each SDPL service provider:

1. has established and maintains detailed documentation covering its:
 - Contingency & Disaster Recovery Plan, including key compromise, hardware, software and communications failures, and natural disasters such as fire and flood;
 - Configuration Baseline, including operating software, anti virus software and PKI specific application programs;
 - backup, archiving and offsite storage procedures;
2. provides the above documentation on the request of:
 - the RCA when conducting a CPS₍₂₎ practices audit;
 - persons conducting a security or compliance audit;
3. provides appropriate training to all relevant staff in contingency and disaster recovery procedures;
4. at least annually tests its Contingency & Disaster Recovery Plan with the minimum test activity being the full restoration of operational services as follows:
 - the current operational platform is shut down and disconnected from communications links;
 - system operating software, application programs and operational data is restored onto a new hardware platform, solely from backup media and in compliance with the Configuration Baseline;
 - the restored service is connected to the communications links and the correct operation of its Certificate services tested;

- service operations are resumed using the original operational platform. All files on the hard disk of the test platform are securely deleted;
- the Contingency & Disaster Recovery Plan is reviewed in the light of the test results.

4.8.1 Computing resources, software, and/or data are corrupted

Each service provider has established a configuration baseline plan, and back-up, archiving and response plan to provide data for identifying component failure and subsequent service restoration.

4.8.2 Entity public key is revoked

Each service provider has established a key and user compromise plan that addresses the actions to be taken in the event that the RCA or CA public key is revoked.

CAs and RAs are to promptly advise the RCA of any compromise or suspected compromise of their private keys.

4.8.3 Entity key is compromised

Each service provider has established a key and user compromise plan that addresses the actions to be taken in the event that a private key is compromised.

4.8.4 Secure facility after a natural or other type of disaster

Each service provider manages its backup, archive and offsite storage in accordance with its configuration baseline plan, and back-up, archiving and response plan.

4.8.5 Contingency & Disaster Recovery Plan

The purpose of this plan is to restore core business operations as quickly as practicable when systems operations have been significantly and adversely impacted by fire, strikes, etc.

The plan should acknowledge that any impact on system operations will not cause a direct and immediate operational impact within the PKI of which the service provider is a part. This means that the plan should have the primary goal of reinstating the service provider platform in order to make accessible the logical records kept within the software. Recovery actions approved within the plan should be given a priority that is in keeping with the recovery of other organisational records that do not have a direct and immediate impact on the organisation's operations.

To implement a Contingency & Disaster Recovery Plan, a service provider:

1. identifies an internal owner for the plan;
2. identifies individuals authorised to initiate disaster recovery action;

3. identifies major elements at risk, for example;
 - operational hardware;
 - CA or RA software application;
 - logical records;
 - RA POI records;
4. identifies criteria that might prompt disaster recovery initiation;
5. implements recommended precautionary measures such as setting up:
 - an Uninterruptable Power Supply;
 - power surge protectors;
6. considers secondary precautionary measures that may be required, such as:
 - a second power supply using an alternate power source;
 - a backup site;
 - trained backup staff;
7. develops recovery actions and timeframes;
8. prioritises recovery actions from most significant to least significant;
9. maintains a record of the hardware and software configuration baseline;
10. maintains records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure, including the intended maximum period that the system is to be down.

To support the disaster recovery plans of associated RAs, CAs will:

1. maintain dedicated hardware specifically for RA disaster recovery support;
2. configure and deliver a new hardware platform to RAs who experience hardware failure.

4.9 CA Termination

When it is necessary to terminate a CA service, the impact of the termination is to be minimised as much as possible in light of the prevailing circumstances. This includes:

1. providing as much prior notice as is practicable and reasonable to:
 - the RCA;
 - all subordinate entities;

2. the progressive transfer of the service, and operational records, to a successor CA;
3. preserving any records not transferred to a successor CA.

4.9.1 Notice

In the case of the programmed termination of a CA, the CA is to provide subordinate RAs with a minimum of eight week's notice of the proposed shut down and of any arrangements that have been made or are to be made for the continuation of services by a successor CA. The subordinate RAs are to promptly advise their End Users, and may be requested to assist in planning the progressive rollout of new keys and Certificates by a successor CA.

In the event of an emergency shut down of a CA, e.g. due to the compromise of the CA's private key, the CA will provide subordinate RAs with as much notice as is practical and reasonable under the prevailing circumstances. All keys and Certificates are to be revoked by the CA immediately and prior to the emergency shut down. Services should be recommenced by the same or a successor CA as quickly as possible after the shut down has been effected.

4.9.2 End User keys and certificates

In the event that it becomes necessary to terminate a CA:

1. all subordinate End User keys and certificates may need to be revoked prior to the shutdown; or
2. all subordinate End User keys and certificates may need to be transferred to a replacement CA, provided the transferred certificates do not become operational within the chain of trust of the replacement CA service until after the shutdown of the terminating CA service; or
3. all End User certificates may need to be revoked prior to the shutdown of the terminating CA service, and the End User keys may be transferred to the replacement CA service for the issue of new certificates, provided that such new certificates are not generated until after the shutdown of the terminating CA service.

Where practical, key and Certificate revocation should be timed to coincide with the progressive and planned rollout of new keys and Certificates by a successor CA.

Compensation or restitution to End Users for the revocation of their Certificates prior to their expiry date is a contractual matter that falls outside the scope of this CPS₍₂₎.

4.9.3 Successor CA CPS₍₁₎

The CPS₍₁₎ under which a successor CA issues Certificates is a contractual matter between the stakeholders and is outside the scope of this CPS₍₂₎. In principle, however, to the extent that it is practical and reasonable:

1. the successor CA should assume the same rights, obligations and duties as the terminating CA;

2. the CPS₍₁₎ under which the successor CA issues Certificates should impose the same requirements and confer the same benefits as the CPS₍₁₎ under which the terminating CA issued Certificates;
3. the successor CA should issue new keys and Certificates to all subordinate service providers and End Users whose keys and Certificates were revoked by the terminating CA due to its termination, subject to the individual service provider or End User making an application for a new Certificate, and satisfying the CPS₍₁₎ initial registration and identification requirements, including the execution of a new service provider or subscriber agreement. Note that section 3.1.11 *Rekey after revocation* prevents the successor CA from renewing Certificates, and that the initial applications by service providers and End Users to the successor CA must be for new Certificates.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

The site location of the SDPL RCA is in a secure office environment at Level 5, 1 James Place, North Sydney NSW Australia.

The RCA operates within a secure physical environment within the office area that meets the standards of an independent security certification body, at a highly protected level.

The site location and construction of CAs operating under the SDPL RCA are detailed in relevant CPS₍₁₎.

5.1.2 Physical access

SDPL permits entry to its secure operating area only to authorised personnel, and to visitors under the constant supervision of an authorised person. The number of personnel authorised to enter the area is kept to a minimum and a log is maintained of all accesses.

CAs within the SDPL hierarchy employ appropriate physical safeguards and work practices to regulate physical access to their secure operating areas, and describe these safeguards and practices in a relevant CPS₍₁₎.

RAs are not required to operate within a secure area, but are obliged to, and do, protect physical access to confidential registration records.

End Users are not to leave their computers unattended when the cryptography is in an unlocked state (i.e., when the password has been entered). A computer that contains private keys encrypted on a hard drive must be physically secured or protected with an appropriate access control product.

5.1.3 Power and air conditioning

The SDPL secure operating area is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

The area has an air conditioning system to control the heat and humidity that is independent of the building air conditioning system.

CAs within the SDPL employ appropriate power supplies and air conditioning systems to protect the uninterrupted provision of their services.

5.1.4 Water exposures

The RCA secure operating area is protected against water exposure by being located on an above ground floor of an office building that is not in a flood zone, and having a built-in six inch raised floor.

All critical components are further protected against water exposure by being contained within waterproof cabinets.

CAs within the SDPL employ appropriate safeguards to protect their secure operating area against water exposure, and describe those safeguards in a relevant CPS₍₁₎.

5.1.5 Fire prevention and protection

Suitable fire extinguishers are maintained in the SDPL secure operating area, to guard against the possibility of fire.

CAs within the SDPL employ appropriate safeguards to protect their secure operating area against fire, and describe those safeguards in a relevant CPS₍₁₎.

5.1.6 Media storage

All magnetic media containing SDPL PKI information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located either within the CA service operations area or in a secure off-site storage area.

5.1.7 Waste disposal

Paper documents and magnetic media containing trusted elements of the SDPL PKI or commercially sensitive or confidential information are securely disposed of by:

1. in the case of magnetic media:
 - physical damage to, or complete destruction of the asset;
 - the use of an approved utility to wipe or overwrite magnetic media;
2. in the case of printed material, shredding, or destruction by an approved service.

5.1.8 Off-site backup

Endorsed off site storage agents are used for the storage and retention of backup software and data.

The off site storage:

1. is available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data;
2. has appropriate levels of physical security in place.

5.2 Procedural Controls

5.2.1 Trusted roles

In order to ensure that one person acting alone cannot circumvent the entire system, responsibilities at a Service Provider workstation are shared by multiple roles and individuals. Oversight may be in the form of a person who is not directly involved in issuing certificates examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy.

This is accomplished by creating separate roles and accounts on the service workstation, each of which has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. At a minimum, the following roles are established:

1. System Administrator;
2. Registrar (RAs only);
3. Security Administrator.

5.2.2 Number of persons required per task

Separate individuals fill each of the three roles described above. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation. However:

1. a single individual may assume the roles of the System Administrator and Registrar;
2. the Security Administrator must always remain separate from the System Administrator in order to provide an independent review of the audit log;
3. any task requiring the creation, backup or importation into a database of a service provider private key must involve two trusted persons, one performing the function and the second fulfilling a security monitoring role.

5.2.3 Identification and authentication for each role

Persons filling trusted roles must undergo an appropriate security screening procedure, designated "Position of Trust".

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The recruitment and selection practices for Service Provider personnel operating under the SDPL PKI take into account the background, qualifications, experience

and clearance requirements of each position, which are compared against the profiles of potential candidates.

5.3.2 Background check procedures

Background checks are conducted on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

5.3.3 Training requirements

All Service Provider staff are trained in:

1. basic PKI concepts;
2. the use and operation of CA or RA software;
3. documented CA and RA procedures;
4. computer security awareness and procedures;
5. for pertinent CA staff, how to explain to RA certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
6. for pertinent RA staff, how to explain to End User certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
7. the meaning and effect of the legal contract their Service Provider has signed with its superior entity;
8. the meaning and effect of relevant CPS₍₁₎, this CPS₍₂₎ and for pertinent RA staff, the subscriber agreement.

5.3.4 Retraining frequency and requirements

SDPL Service Provider staff receive a security briefing update at least once a year.

Training in the use and operation of CA or RA software is provided when new versions of the software are installed.

Remedial training is completed when recommended by audit comments.

5.3.5 Job rotation frequency and sequence

SDPL service providers may implement formal job rotation practices (e.g. through formal reliefs). Where formal job rotation is not implemented, cross-training activities are conducted to ensure operations continuity.

5.3.6 Sanctions for unauthorized actions

Unauthorised actions by SDPL Service Provider staff are submitted to appropriate authorities including, but not limited to, the Security Administrator.

5.3.7 Contracting personnel requirements

SDPL Service Provider staff may be contractors who are appointed in writing and given written notification of the terms and conditions of their position. They are normally assigned full-time to their Service Provider responsibilities.

5.3.8 Documentation supplied to personnel

SDPL Service Provider staff have access to all relevant:

1. hardware and software documentation;
2. Service Provider:
 - application manuals;
 - policy documents, including relevant CPS₍₁₎;
 - operational practice and procedural documents, including this CPS₍₂₎;

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Service Provider key pairs are generated and installed by the relevant Service Provider.

End User key pairs may be generated by an authorised RA or by the End Users, and are installed by the End User.

6.1.2 Private key delivery to entity

Self-generated private keys do not require delivery.

Where an End User's private keys are generated by an RA, they are delivered using one of a variety of secure delivery methods, including but not limited to delivery by e-mail, floppy disk or FTP transfer. A key transport access control mechanism may be used.

6.1.3 Public key delivery to certificate issuer

Public keys are delivered to the certificate issuer by means of a protected on-line exchange utilising automatic functions of the Service Provider application software.

The RCA's public keys do not require delivery, since the RCA generates its own keys and self-signs its certificates.

6.1.4 CA public key delivery to users

The Service Provider public keys required by an End User may be distributed with the End User's own keys and certificates or may be downloaded by the End User from the SDPL X.500 Directory.

6.1.5 Key sizes

Key lengths within the SCPL PKI are determined by Certificate profiles and are detailed in a relevant CPS₍₁₎. They are typically a minimum of 1024 bits.

6.1.6 Public key parameters generation

The parameters used to create public keys are generated by the relevant Service Provider application, except for self-generated End User keys in which case the parameters are generated by the End User's client application.

6.1.7 Parameter quality checking

The quality of public key parameters is automatically checked by the Service Provider application that generates the key, except for self-generated End User keys in which case the parameters are quality checked by the RA prior to submitting a certification request to the CA.

6.1.8 Hardware/software key generation

Service Provider and End User key generation may be performed in hardware or software.

6.1.9 Key usage purposes

Keys may be used for the purposes and in the manner described in section 1.3.4 *Applicability* of a relevant CPS₍₁₎. Any restrictions described in the section must be observed.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

Cryptographic modules in use within the SDPL PKI comply with industry standards.

6.2.2 Private key (n out of m) multi-person control

Private keys may be under n out of m multi-person control as prescribed in a relevant CPS₍₁₎.

6.2.3 Private key escrow

Private key escrow is not supported.

6.2.4 Private key backup

Service Provider private keys are stored in an encrypted database, which is backed up under further encryption with backup copies maintained on site and in secure off site storage.

End Users may choose to backup their private keys by backing up their hard drive or the encrypted file containing their keys.

6.2.5 Private key archival

See section 4.6.2.1 *Secure maintenance of keys*.

6.2.6 Private key entry into cryptographic module

If a cryptographic module is used, the private key must be generated in it and remain there in both encrypted and decrypted forms, and be decrypted only at the

time at which it is being used.

6.2.7 Method of activating private key

Private keys are activated by the Service Provider application or the End User Client application, following the successful completion of a login process which requests and validates an authorised user password.

6.2.8 Method of deactivating private key

Private keys are de-activated when the Service Provider application or End User Client application is terminated.

6.2.9 Method of destroying private key

Service Provider applications do and End User Client applications must destroy private keys in memory by overwriting them with zeros when the application shuts down.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

All public keys are archived by the certifying CA.

6.3.2 Usage periods for the public and private keys

As prescribed within a relevant CPS₍₁₎.

6.4 Activation Data

6.4.1 Activation data generation and installation

No activation data other than access control mechanisms is required to operate cryptographic modules.

An End User Personal Identification Code (PIC) may be generated by an RA during key pair creation, to protect the transport of an End User's keys and certificates to the End User.

6.4.2 Activation data protection

No activation data other than access control mechanisms is required to operate cryptographic modules.

PICs may be supplied to End Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third party interception of the PIC.

6.4.3 Other aspects of activation data

Where a PIC is used, the End User is required to enter the PIC and identification details such as their distinguished name before they are able to access and install their keys and certificates.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

Each SDPL Service Provider has established an approved System Security Plan that incorporates computer security technical requirements that are specific to that Service Provider's operations.

6.5.2 Computer security rating

Each SDPL Service Provider has established an approved System Security Plan that incorporates computer security ratings that are specific to that Service Provider's operations.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

Service Provider and End User Client applications are developed in controlled environments employing appropriate quality controls.

6.6.2 Security management controls

System security management is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in section 5.2.1 *Trusted roles*.

6.6.3 Life cycle security ratings

Each SDPL Service Provider has established an approved Protective Security Risk Review that identifies and addresses all high or significant life cycle security threats.

6.7 Network Security Controls

Each SDPL Service Provider has established an approved Protective Security Risk Review that identifies and addresses all high or significant network security threats.

6.8 Cryptographic Module Engineering Controls

Each SDPL Service Provider has established an approved Protective Security Risk Review that identifies and addresses all high or significant cryptographic module engineering security threats.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

The SDPL PKI supports and uses X.509 Version 3 certificates, which contain v.3 in the version field.

7.1.2 Certificate extensions

The SDPL PKI supports and uses X.509 Version 3 certificate extensions.

7.1.3 Algorithm object identifiers

OIDs are not allocated to algorithms supported and used within the SDPL PKI.

The following hashing/digest algorithms are supported:

1. Secure Hash Algorithm-1 (SHA-1)
2. Message Digest 5 (MD5)

The following padding algorithms are supported:

1. ISO 9796
2. PKCS#1

The following encryption algorithms are supported:

1. RSA
2. DES

The use of multiple algorithms within the same hierarchy is supported.

7.1.4 Name forms

Certificates issued by the SDPL PKI contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields.

7.1.5 Name constraints

Anonymous names are not supported. Pseudonymous names that may cause offence are not permitted.

7.1.6 Certificate policy Object Identifier

CPS₍₁₎ OIDs are carried in the standard extension field of SDPL PKI X.509 certificates and published in the relevant CPS₍₁₎.

7.1.7 Usage of Policy Constraints extension

The use of the Policy Constraints extension is supported.

7.1.8 Policy qualifiers syntax and semantics

The use of syntax and semantics policy qualifiers is supported.

7.1.9 Processing semantics for the critical certificate policy extension

See section 1.1.2.1 X.509 *Certificate extensions*.

7.2 CRL Profile

7.2.1 Version number(s)

The SDPL PKI supports and uses X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

The SDPL PKI supports and uses X.509 Version 2 CRL entry extensions.

8. SPECIFICATION ADMINISTRATION

SDPL operates a Policy Approval Authority which is responsible for setting Certificate policy direction for the overall public key infrastructure. Contact details for the PAA appear in each CPS₍₁₎ applicable to the SDPL hierarchy.

A Policy Creation Authority is normally vested at the CA or equivalent level in a PKI hierarchy. In the case of the SDPL PKI, the PAA and PCA functions are vested in the same authority, the PAA.

Each CPS₍₁₎ used under the SDPL hierarchy has been allocated an OID which:

1. provides a unique identification for the CPS₍₁₎;
2. includes a policy version number.

8.1 Specification change procedures

Initial publication

The PAA is the responsible authority for changes to a CPS₍₁₎. New CAs apply to the PAA for:

1. formal endorsement of the CPS₍₁₎ under which they will issue Certificates;
2. the allocation of an OID.

After the CPS₍₁₎ has been approved and the OID has been granted, the CA:

1. publishes, on a nominated web site, the CPS₍₁₎ together with this CPS₍₂₎;
2. advises all subordinate parties of the CPS₍₁₎ and its applicability;
3. forwards a copy of the CPS₍₁₎ to each subordinate RA, together with an advice regarding the web site of the master CPS₍₁₎.

8.1.1 Change

There are two possible types of policy change:

1. the issue of a new CPS₍₁₎;
2. a change to or alteration of an existing policy.

If an existing policy requires re-issue, the change process employed is the same as for as for initial publication, as described above. Note that the new OID issued for a policy change differs from the previous OID only in the policy version number.

8.2 Publication and notification policies

New or amended CPS₍₁₎ are published on the web site nominated in the CPS₍₁₎.

Subordinate parties are notified by the appropriate CA of changes to a CPS₍₁₎ as and when they are approved. Subordinate CAs and RAs are advised of the changes a minimum of one week prior to publication.

8.3 CPS approval procedures

CPS₍₁₎ intended for use under the SDPL RCA must be endorsed by the SDPL PAA. A document setting out the functions of the SDPL RCA PAA is made available to all subordinate parties responsible for creating or amending CPS₍₁₎, the document is also made available to any approved person conducting a security audit.

9. Appendix A - Glossary

Term or Acronym	Explanatory notes
Access	Obtaining knowledge or possession of classified material, or access to a designated secure area.
Access control list*	A list of entities, together with their access rights, which are authorised to have access to a resource.
Access control*	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.
Accountability*	The property that ensures that the actions of an entity may be traced uniquely to the entity.
ACSI	Australian Communications - Electronic Security Instruction.
Administrative Security	Any procedural system that is established to ensure that classified material or valuable asset is protected against loss, damage or unauthorised access.
Adverse Security Assessment	A security assessment in respect of a person that contains: <ul style="list-style-type: none"> (a) any opinion or advice or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person; and (b) a recommendation that prescribed administrative action be taken or not be taken in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person.
Agency	Generic term used to describe all Commonwealth Government entities. Any Australian Government department, authority, agency or other body established in relation to public purposes.
Agency Assessment / Recommendation	The final interpretation formulated by the agency of the results of all checking and assessment action - including the ASIO Security Assessment, where sought culminating in a recommendation to the Agency Head or his/her delegate to grant, withhold, continue, rescind, or otherwise vary a proposed or existing security clearance.
Agency Evaluation	The assessment by agency security personnel, prior to submission of any request to ASIO for a Security Assessment, of the results of all checking and character assessment action, with a view to determining in consultation with agency management whether or not to cease all such action, consult with ASIO, and/or proceed with further clearance action, including for DSAPs submitting a request to ASIO for a Security Assessment (with or without a memorandum of information of possible security significance obtained through agency checking action, as deemed appropriate).
Agency Head	Means the head of a Department of State or a Department of the Public Service or the Chief Executive Officer of any other authority or agency of the Australian Government, including the Chief of the Defence Force, and the Chiefs of Staff for the Navy, Army and Air-Force.
Agency Security Advisers	That person nominated by the Agency Head to perform the day-to-day protective security functions within his/her agency.
Agency Security Instructions	Instructions issued by an Agency providing protective security policy and procedural advice to all staff within that agency. These instructions should preferably be issued under the authority of the Agency Head.
AISEF	Australasian Information Security Evaluation Facility

Term or Acronym	Explanatory notes
AISEP	Australasian Information Security Evaluation Program
ANAO	Australian National Audit Office
ASIO	The Australian Security Intelligence Organisation.
Asset*	Anything that has value to the organisation.
Assets*	Information or resources to be protected by technical or non technical countermeasures of a TOE.
Assurance*	Confidence that an entity meets its security objectives.
ASVS	Australian Security Vetting Service
Asymmetric authentication method*	A method of authentication, in which not all authentication information is shared by both entities.
Asymmetric cryptographic technique*	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. NOTE - A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature schemes, encipher and decipher for encipherment systems. The signature and decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, since this is not the general case, throughout this International Standard the four elementary transformations and the corresponding keys are kept separate.
Asymmetric encipherment system*	A system based on asymmetric techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment.
Asymmetric key pair*	A pair of related keys where the private key defines the private transformation and the public key defines the public transformation.
Asymmetric signature system*.	A system based on asymmetric techniques whose private transformation is used for signing and whose public transformation is used for verification.
Authenticated identity*	A distinguishing identifier of a principal that has been assured through authentication.
Authentication	The process whereby a service provider satisfies him/her self to an appropriate level of confidence that a service requester is entitled to the service sought.
Authentication certificate*	A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.
Authentication data*	Information used to verify the claimed identity of a subject
Authentication exchange*	(i) A mechanism intended to ensure the identity of an entity by means of information exchange. (ii) Information used for authentication purposes.
Authentication initiator*	The entity that starts an authentication exchange.

Term or Acronym	Explanatory notes
Authentication private key	The key used to digitally sign a message.
Authentication public key	The key used to verify a digital signature.
Authentication token (token)*	Information conveyed during a strong authentication exchange, which can be used to authenticate its sender.
Authentication*	The provision of assurance of the claimed identity of an entity.
Authenticity*	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
Authorised	Authorised by the Agency Head or his/her delegate.
Authorised administrator*	A user to whom authorisation has been granted to perform administrative operations which may affect the enforcement of the TSP.
Authorised user*	A user who may, in accordance with the TSP, perform an operation
Authorisation*	The granting of rights, which includes the granting of access based on access rights.
Background Checking	That activity which is concerned primarily with verification of the personal, family, and other details stated in forms and related documents completed by an individual under consideration for possible employment in a Position of Trust (POT).
Biometrics	Technology that measures a presented human anatomical part and which then compares that against a known measure. e.g. fingerprint comparison.
CA	Certification Authority.
Cabinet Document	Those documents as defined and described in the Cabinet Handbook.
CASP	A Certification Authority Service Provider.
CBC	Cipher Block Chaining
Certificate ⁴	A set of information which at least: <ul style="list-style-type: none"> - identifies the Certification Authority issuing the certificate; - unambiguously names or identifies its owner; - contains the owners public key; and - is digitally signed by the Certification Authority issuing it.
Certificate (user certificate)*	The public keys of a user, together with some other information, rendered unforgeable by encipherment with the secret key of the certification authority which issued it.
Certificate of Accreditation	A certificate issued by the GPKA endorsing the holder to provide CA services to users on behalf of an agency.
Certificate Policy Statement (CPS ₍₁₎)	The suite of policies that support a Certification Authority in generating certificates and the binding of certificates to an individual.
Certificate Practice Statement (CPS ₍₂₎)	A statement of the practices that a Certification Authority employs in issuing certificates.

⁴ Definition from SAA MP75 (Standards Australia).

Term or Acronym	Explanatory notes
Certificate Revocation List (CRL)	<p>The process of retracting the guarantees associated with a public key pair. In particular the guarantee that the entity and the public key pair are mutually identified bound. Revocation may occur where a public key pair:</p> <ul style="list-style-type: none"> - has been compromised; - has outlived its intended life; - is no longer fit for purpose; - use has been proven to be fraudulent; - at the request of the owner; - in accordance with the policies of the CA
Certificate serial number*	An integer value, unique within the issuing CA (certification authority), which is unambiguously associated with a certificate issued by that CA.
Certificate*	An entity's data rendered unforgeable with the private or secret key of a certification authority.
Certification authority (CA)*	<p>(i) A centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities.</p> <p>(ii) An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the user's keys.</p> <p>(iii) A trusted entity that verifies the identity of a user, allocates a Distinguished Name to that user, and verifies the correctness of information concerning that user by signing the data which constitutes the digital signature for that user.⁵</p>
Certification chain	See Certification path
Certification path*	An ordered sequence of certificates of objects in the DIT (directory information tree) which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path
Certification Request	means an electronic document containing the details of the Certificates which are to be created by the CA, completed and digitally signed by the RA, and sent by the RA to the CA.
CGIO	Chief Government Information Officer
Character Assessment	<p>The balanced and informed estimation of an individual's reliability and trustworthiness which is derived from comprehensive checks on identity, background, personal values and behaviour.</p> <p>Checks of Police Records are an integral part of this activity.</p>
Classified Material	<p>Official information which, for reasons of security, requires protection to prevent its being acquired by people, organisations or governments not authorised to receive it.</p> <p>Classified material may be either 'national security' or 'non national security' material.</p>
Commonwealth Contractor	A person performing work or rendering services for a Commonwealth agency, other than as a employee of the agency, including a person performing such services as a sub-contractor or as an adviser or consultant.

⁵ Ibid.

Term or Acronym	Explanatory notes
Communications Security (COMSEC)	All measures applied to the protection of telecommunications from unauthorised interception and exploitation. Communications Security includes: <ul style="list-style-type: none"> (a) Crypto security - That component of communications security which results from the provision of technically sound cryptosystems and their proper use; (b) Physical security - That element of communications security which results from all physical measures necessary to safeguard classified equipment, material and documents from access or observation by unauthorised people; and (c) Transmission Security - That component of communication security which results from all measures designed to protect transmissions from unauthorised interception, traffic analysis and imitative deception (the latter term relates to attempts to introduce bogus transmissions into a communications system).
Concept Of Operations (CONOPS)	A high level description of the process or procedures under which a system operates. Includes a description of inputs, processing and outputs.
Confidentiality private key	The key used to decipher or decode the contents of a message.
Confidentiality public key	The key used to encipher or encode the contents of a message.
Confidentiality*	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
CONOPS	See Concept of Operations.
COTS	Commercial off the shelf product
CPS ₍₁₎	See Certificate Policy Statement.
CPS ₍₂₎	See Certificate Practice Statement.
Credentials*	Data that is transferred to establish the claimed identity of an entity.
CRL	Certificate Revocation List
Cross certification	Practice of mutual recognition of another CAs certificates to an agreed level of confidence. Usually evidenced in contract. GPKA endorsed CAs shall only cross certify with other GPKA CAs.
Cryptographic algorithm*	A cryptographic algorithm is defined as an algorithm which transforms data in order to hide or reveal its information content and which uses at least one secret parameter. This definition includes both symmetric algorithms (e.g. DES and FEAL) and asymmetric algorithms (e.g. RSA and Rabin). In the case of a symmetric algorithm the data is hidden and revealed using a secret parameter. In the case of an asymmetric algorithm the data is hidden using a public parameter and revealed using a secret parameter.
Cryptographic equipment*	Equipment in which cryptographic functions (e.g. encipherment, authentication, key generation) are performed.
Cryptographic Information	Information, including crypto-material, significantly descriptive of cryptographic techniques and processes, or of cryptosystems and equipment or their functions and capabilities, the disclosure of which would assist the cryptanalytic solution of an encrypted text or a crypto-system.
Cryptographic key; key*	A parameter used in conjunction with an algorithm for the purpose of validation, authentication, encipherment or decipherment.

Term or Acronym	Explanatory notes
Cryptography*	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.
DAP	Directory Access Protocol
Data integrity*	The property that data has not been altered or destroyed in an unauthorised manner.
Data storage*	A means for storing information from which data is submitted for delivery, or into which data is put by the delivery authority
Data string (data)*	The string of bits which is the input to a hash-function.
DEA	Data Encryption Algorithm
Decrypt	Practice of recovering an encrypted message by reverting from cipher text to plain language.
Defence Signals Directorate	The Commonwealth authority in matters pertaining to communications and computer security. It is located within the Department of Defence.
DES	Data Encryption Standard
Digest	The result from the application of a hashing algorithm to message text to a defined data. It is just a quotient.
Digital signature ⁶	A digital signature is a mathematical construct that creates a unique and unforgeable identifier of the owner of the Distinguished Name.
Digital signature*	Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient
Director General	The Director General of Security holding office under the ASIO Act 1979 (i.e. the Head of ASIO).
Directory	An online database containing public keys, Public Key Certificates and CRLs.
DISP	Defence Industrial Security Program.
Document	Anything on which information is recorded by any means, including words, symbols, images or electro-magnetic impressions.
DSA	Digital Signature Algorithm. Directory Service Agent.
DSD	Defence Signals Directorate.
DSS	Digital Signature Standard.
Dual control*	A process of utilising two or more separate entities (usually persons), operating in concert, to protect sensitive functions of information whereby no single person is able to access or utilise the materials, e.g. cryptographic key.
EDI	Electronic Data Interchange.
EDP	Electronic Data Processing.
Emergency Key Recovery	A method for retrieving private confidentiality keys from an authorised archive in an emergency.
Enablers	Small applications that allow a user to access and use a public key in an electronic service.
Encrypt	Practice of converting plain language to cipher text.

⁶ Ibid.

Term or Acronym	Explanatory notes
End User	Means a party who has been issued with private keys and Certificates under the terms of a recognised policy, who receives or relies on cryptographic keys to authenticate themselves, or another End User, and/or to protect confidential information.
Entity authentication*	The corroboration that an entity is the one claimed.
EPL	DSD Evaluated Products List (List of products that have undergone a review process through the national authority.)
Evaluation authority*	A body which implements the criteria for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
Evaluation scheme*	The administrative and regulatory framework under which the criteria are applied by an evaluation authority within a specific community.
Evaluation*	Assessment of an IT system or product against defined criteria.
Explicit key authentication to A*	The assurance for one entity A that only another identified entity is in possession of the correct key. NOTE - Implicit key authentication to A and key confirmation to A together imply explicit key authentication to A.
GATEKEEPER	Project name for the implementation of a whole of Government Public Key Infrastructure.
GOLD	Government On Line Directory.
GPKA	Government Public Key Authority.
GPKI	Government Public Key Infrastructure.
Hash	A computed number. A hash is used to compare versions of a calculated piece of data. If the hash results match, an assurance can be drawn that the data has not been tampered with.
Hash field*	Field of the intermediate string which conveys the hash-code.
Hash function*	<p>(i) A (mathematical) function which maps values from a (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range.</p> <p>(ii) A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:</p> <ul style="list-style-type: none"> - it is computationally infeasible to find for a given output an input which maps to this output. - it is computationally infeasible to find for a given input a second input which maps to the same output. <p>[ISO/IEC 10118-1: 1994] [FCD ISO/IEC 14888-1 (12/1997)] The following notes are contained in ISO/IEC 10118-1. The second note is also contained in ISO/IEC 14888-1.</p> <p>NOTES</p> <ol style="list-style-type: none"> 1. The literature of the subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples. 2. Computational feasibility depends on the user's specific security requirements and environment.
Hash-code*	The string of bits which is the output of a hash-function.

Term or Acronym	Explanatory notes
Head Agreement	Contractual instrument for the provision of Whole Of Government Telecommunications services.
HIC	Health Insurance Commission
Hierarchy	See SDPL PKI Hierarchy
HIGHLY PROTECTED	The highest level of non national security classification.
HTTP	Hypertext Transfer Protocol
ICA	Intermediate Certification Authority - An entity on the second level of the PKAF hierarchy and which is immediately subordinate to the PARRA
Identification data*	<p>(i) A sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it. NOTE - Examples of data items which may be included in the identification data include: an account number, expiry date, serial number, etc.</p> <p>(ii) A sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it. NOTE - The identification data may additionally contain data items such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters. [FCD ISO/IEC 14888-1 (12/1997)]</p>
Identity*	A method for identifying the user, which can either be the real name of that user or a pseudonym. [2 nd CD ISO/IEC 15408-1 (11/1997)]
Identity-based security policy*	A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed.
IMAP	Information Management Access and Policy Branch
-IN-CONFIDENCE-	The classification given to material and resources, other than national security classified information or Cabinet documents, which require a limited degree of protection (i.e. the lowest level of non national security classification).
ISO	International Organisation for Standardisation
IT security policy*	Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organisation and its IT systems.
IT security*	All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.
IT/12/4/1	Standards Australia Committee for PKAF related standards
ITSEC	Information Technology Security Evaluation Criteria
Key establishment*	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
Key generating function*	A function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm and application. The function shall have the property that it shall be computationally infeasible to deduce the output without prior knowledge of the secret input.
Key generator*	A type of cryptographic equipment used for generating cryptographic keys and, where needed, initialisation vectors.

Term or Acronym	Explanatory notes
Key management*	The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.
Key pair	Expression used to describe the public and private keys of Public Key Technology
Key token*	Key management message sent from one entity to another entity during the execution of a key management mechanism
Key transport*	The process of transferring a key from one entity to another entity, suitably protected
Key*	(i) A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification). (ii) A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment).
Keying material*	The data (e.g. keys, initialisation values) necessary to establish and maintain cryptographic keying relationships
LDAP	Lightweight Directory Access Protocol
Masquerade*	The pretence by an entity to be a different entity.
Message*	(i) String of bits of limited length. (ii) A string of bits of any length. (iii) String of bits of any length, possibly empty.
Message authentication code (MAC)*	(i) A code in a message between a sender and a receiver used to validate the source and part or all of the text of a message. The code is the result of an agreed calculation. (ii) A data item derived from a message using symmetric cryptographic techniques and a secret key. It is used to check the integrity and origin of the message by any entity holding the secret key.
MOA	Memorandum Of Agreement
Monitor (Monitoring Authority)*	A trusted third party monitoring the actions and events and trusted to provide evidence about what was monitored.
MOU	Memorandum Of Understanding
NATA	National Association of Testing Authorities
National Security Classifications	Those classifications used to designate classified national security material. The classifications are TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED.
National Security Clearance	A clearance issued by an agency to enable a person to have access to national security material or a designated secure area.
National Security Material	Material in any form pertaining to Australia's security and defence, to some international relations and some matters affecting the national interests.
Need-to-Know	A criterion which requires the custodian of classified matter to establish, prior to disclosure, that the intended recipient needs access to the material to perform his/her official duties.
NOIE	National Office of the Information Economy.
Non-repudiation exchange*	A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation.

Term or Acronym	Explanatory notes
Non-repudiation information*	A set of information that may consist of the information about an event or action for which evidence is to be generated and validated, the evidence itself, and the non-repudiation policy in effect.
Non-repudiation policy*	A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.
Non-repudiation token*	A special type of security token as defined in ISO/IEC 10181-1 consisting of evidence, and, optionally, of additional data.
NRT token*	Non-repudiation of transport token. A data item which allows either the originator or the delivery authority to establish non-repudiation of transport for a message.
OCA	Organisation Certification Authority.
OECD	Organisation for Economic Co-operation and Development.
OGO	Office of Government Online.
ORA	Organisation Registration Authority – An entity which establishes the identities of subordinate users and registers their certification requirements with a Certification Authority.
Organisational security policy*	A set of security rules, procedures, practices, and guidelines imposed by an organisation upon its operations.
PAA	Policy Approval Authority.
PARRA	Policy and Root Registration Authority – An entity which creates and monitors compliance with the overall guidelines that all users, associations of users, tiered levels of Certification Authorities and subordinate policy making authorities must follow.
Personal Identification Code	An access control mechanism used during key transport to import private keys into an End User application.
Personnel Security	The protective measures used to ensure that only suitable people are given access, remain suitable for access and are made aware of their security responsibilities.
Physical Security	(i) That part of protective security concerned with physical measures designed to prevent unauthorised access to resources, and to safeguard them against espionage, deliberate damage, alteration or theft (e.g. locks, alarms, safes, etc). (ii) The measures used to provide physical protection of resources against deliberate and accidental threats.
PIC	See Personal Identification Code.
PKAF	Public Key Authentication Framework – A framework that, if followed, allows for the establishment of a trusted public key system. This system will allow any entity to determine the trust and validity of a digital signature claimed to be associated with another entity.
PKI	Public Key Infrastructure.
PKT	Public Key Technology.
POI	Proof of Identity.
Police Records Checks	A check, in the proper form, of records of police forces for any conviction, charges pending or other criminal activity regarding the vettee.

Term or Acronym	Explanatory notes
Position of Trust (POT)	A position on the establishment of an agency the duties of which are likely to involve access to sensitive material, and/or valuable or attractive resources, or a position in which the occupant may exercise considerable authority/responsibility – e.g. the granting of major contracts.
Position of Trust Clearance	A clearance issued by an Agency to enable a person to have access to sensitive material or resources of a valuable or attractive nature.
Preferred Candidate	The candidate for appointment, promotion, transfer to a designated security assessment position or position of trust who, subject to the granting of a clearance, will be appointed, promoted or transferred to the position.
Privacy*	The right of individuals to control or influence what information related to them may be collected and stored and to whom that information may be disclosed. NOTE - Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.
Private key*	<ul style="list-style-type: none"> (i) Secret part, key or mathematical construct from a pair of keys which together form the basis of Public Key Technologies. (See Public key) (ii) That key of an entity's asymmetric key pair which shall normally only be known by that entity. NOTE - In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation. [2nd DIS ISO/IEC 11770-3 (08/1997)] 13888-1: 1997 (iii) That key of an entity's asymmetric key pair which is usable only by that entity. In the case of an asymmetric signature system, the private key and the associated algorithms define the signature transformation. (iv) (secret key - deprecated) (In a public key cryptosystem) that key of a user's key pair which is known only by that user. (v) That key of an entity's asymmetric key pair which should only be used by that entity. The following note is contained in ISO/IEC 9798-1: NOTE - In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation. The following note is contained in ISO/IEC 11770-1: NOTE - A private key shall normally not be disclosed.
Private signature key*	Private key which defines the private signature transformation. NOTE - This is sometimes referred to as a secret signature key.
PROTECTED	The classification applied to sensitive material requiring a reasonable degree of protection (i.e. the middle sensitive material classification).
Protective Security	The total concept of administrative, personnel, physical, technical, computer and communication security.
PSM	Protective Security Manual
PSRR	Protective Security Risk Review

Term or Acronym	Explanatory notes
Public key*	<p>(i) Public part, key or mathematical construct from a pair of keys which together form the basis of Public Key Technologies. (See Private key) The key of an entity's asymmetric key pair which can be made public. In the case of an asymmetric signature system, the public key and the associated algorithms define the verification transformation. [ISO/IEC 13888]</p> <p>(ii) (In a public key cryptosystem) that key of a user's key pair which is publicly known. [ISO/IEC 9594-8:1990] [CCITT X.509: 1988]</p> <p>(iii) That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1 (2nd edition): 1997] [ISO/IEC 11770-1: 1997] [2nd DIS ISO/IEC 11770-3 (08/1997)] The following note is contained in ISO/IEC 9798-1 and in ISO/IEC 11770-3: NOTE - In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.</p>
Public key certificate (certificate)*	<p>(i) The public key information of an entity signed by the certification authority and thereby rendered unforgeable. [ISO/IEC 9798-1 (2nd edition): 1997] [ISO/IEC 11770-1: 1997] [2nd DIS ISO/IEC 11770-3 (08/1997)]</p> <p>(ii) A security certificate which binds unforgeably the public key of an entity to the entity's distinguishing identifier, and which indicates the validity of the corresponding private key. [ISO/IEC]</p>
Public key derivation function*	<p>A public function, which maps strings of bits to positive integers, which is used to transform an entity's identification data to its verification key, and which satisfies the following two properties:</p> <ul style="list-style-type: none"> - It is computationally infeasible to find any two distinct inputs which map to the same output. - Either the probability that a randomly chosen value Y is in the range of the function is negligibly small, or it is computationally infeasible to find for a given output an input which maps to this output. <p>NOTE - Negligibility and computational infeasibility depend on the user's specific security requirements and environment.</p>
Public key information*	<p>(i) Information specific to a single entity and which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms.</p> <p>(ii) Information containing at least the entity's distinguished identifier and public key. The public key information is limited to data regarding one entity, and one public key for this entity. There may be other static information regarding the certification authority, the entity, the public key, or the involved algorithms, included in the public key information.</p>

Term or Acronym	Explanatory notes
Public key information*	<p>(i) Information specific to a single entity and which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms.</p> <p>(ii) Information containing at least the entity's distinguished identifier and public key. The public key information is limited to data regarding one entity, and one public key for this entity. There may be other static information regarding the certification authority, the entity, the public key, or the involved algorithms, included in the public key information.</p>
Public verification key*	Public key which defines the public verification transformation.
Qualified Security Assessment	<p>A security assessment in respect of a person that:</p> <p>(a) contains any opinion or advice, or any qualification of any opinion or advice, or any information, that is or could be prejudicial to the interests of the person; and</p> <p>(b) does not contain a recommendation of the kind referred to in paragraph (b) of the definition of "adverse security assessment", whether or not the matters contained in the assessment would, by themselves, justify prescribed administrative action being taken or not being taken in respect of the person to the prejudice of the interests of the person.</p>
RA	Registration Authority.
RCA	Root Certification Authority.
Recipient*	The entity that gets (receives or fetches) a message for which non-repudiation services are to be provided.
Registration	Process of establishing the identity of an individual and documentation of proof to a prescribed level of confidence.
Registration Authority	Registration Authority – An entity which establishes the identities of users and registers their certification requirements with a Certification Authority
Repudiation*	Denial by one of the entities involved in a communication of having participated in all or part of the communication
Resource	Personnel, property or information belonging to, or in the care of an agency.
RESTRICTED	The classification allocated to national security information the unauthorised disclosure of which could possibly be harmful to the national security.
Risk analysis*	The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.
Risk management*	The total process of identifying, controlling, and eliminating or minimising uncertain events that may affect IT system resources.
Risk*	The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.
Role*	A predefined set of rules establishing the allowed interactions between a user and the TOE
RSA	Rivest Shamir Adleman
SDPL PKI Hierarchy	The PKI infrastructure which consists of, at its apex the Security Domain Pty Limited (SDPL) Root Certification Authority under which subordinate elements identified by Object Identifiers (OID) may exist which in turn may have further subordinate OID.

Term or Acronym	Explanatory notes
Signature key*	A secret data item specific to an entity and usable only by this entity in the signature process.
SOP	Standard Operating Procedures
SSP	System Security Plan
Standards Australia	An Australian organisation whose mission is to develop and promote the use of standards.
Steering Committee	Peak directional committee for Project GATEKEEPER
Subordinate CA	A CA that is underneath another CA higher in the trust hierarchy.
Symmetric authentication method*	A method of authentication in which both entities share common authentication information.
Symmetric cryptographic technique*	A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.
System integrity*	The property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system.
Target of Evaluation (TOE)*	An IT product or system and its associated administration and user guidance documentation that is the subject of an evaluation
Threat*	(i) A potential event that could adversely affect the status of a resource, such as through loss, damage, destruction, reduced capacity, compromise, etc. (ii) A potential violation of security. (iii) A potential cause of an unwanted incident which may result in harm to a system or organisation.
Threat Assessment	A judgement of the likelihood or probability of an event taking place that could adversely affect an agency's resources.
TOE resource*	Anything useable or consumable in the TOE.
TOE Security Policy (TSP)*	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
Token*	A message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique.
TOP SECRET	The classification allocated to national security information the unauthorised disclosure of which could cause exceptionally grave damage to the national security. It is the highest national security classification.
Trusted path*	A means by which a User and a TSF can communicate directly with necessary confidence to support the TSP.
Trusted third party*	(i) A security authority, or its agent, trusted by other entities with respect to security related activities. In the context of this multipart standard, a trusted third party is trusted either by the originator, the recipient, and/or the delivery authority for the purposes of non-repudiation, and by another party such as the adjudicator. (ii) A security authority, or its agent, trusted by other entities with respect to security related activities.
TSA	Time Stamp Authority.
TTP	Trusted Third Party.

Term or Acronym	Explanatory notes
User	Any entity (human or machine) outside the TOE that interacts with the TOE.
Validation*	The process of checking the integrity of a message, or selected parts of a message.
Verification authentication information (verification AI)*	Information used by a verifier to verify an identity claimed through exchange AI.
Verification key*	(i) A value required to verify a cryptographic check value. (ii) A data item which is mathematically related to an entity's signature key and which is used by the verifier in the verification process.
Verification process*	A process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid.
Verifier*	(i) An entity that verifies an evidence. (ii) An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.
Vetting	The process of acquiring information to assess a person's suitability for access to classified and/or sensitive material or to a designated secure area.
WEMA	World Electronic Messaging Association.
Word*	A string of 32 bits.

NOTE: Terms or acronyms marked (*) have been adopted from ISO draft (subject to change) Glossary of IT security terminology prepared by JTC1 SC 27 at:

<http://www.iso.ch.8080/jtc1/sc27/27sd698a.htm>

5. Appendix B – CPS₍₁₎ Supported under this CPS₍₂₎

The following CPS₍₁₎ are supported under this CPS₍₂₎:

1. SDPL RCA CPS₍₁₎;
2. SDPL CA CPS₍₁₎;
3. SDPL Demonstration CA (DCA) CPS₍₁₎;
4. SDPL Individual Certificates CPS₍₁₎;
5. SDPL Organisation Certificates CPS₍₁₎;
6. SDPL Employee Certificates CPS₍₁₎.