



SECURITY DOMAIN

Baltimore Certificates On-Line

SDPL P10 (A1 –01) SDPL RCA CPS₍₁₎

Information in this document is subject to change without notice.

No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from Security Domain Pty Limited.

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

Copyright © 1998, 1999 Security Domain Pty Limited,
ACN 82074575.

All Rights Reserved.

TABLE OF CONTENTS

SDPL RCA CPS ⁽¹⁾	7
1. INTRODUCTION.....	8
1.1 Overview	8
1.1.1 Standards	8
1.1.2 Certificate types issued	8
1.1.3 Definitions.....	9
1.2 Identification.....	9
1.2.1 X500 Object Identifier hierarchy	9
1.2.2 SDPL RCA OID	9
1.2.3 SDPL RCA CPS ⁽¹⁾ OID.....	9
1.3 Community and Applicability	9
1.3.0 Policy Authorities	10
1.3.1 Certification authorities	11
1.3.2 Registration authorities.....	11
1.3.3 End entities	11
1.3.4 Applicability	12
1.4 Contact Details	12
1.4.1 Specification administration organization.....	12
1.4.2 Contact person	12
1.4.3 Person determining CPS suitability for the policy	12
2. General Provisions	13
2.1 Obligations.....	13
2.1.0 SDPL Obligations.....	13
2.1.1 CA Obligations.....	13
2.1.2 RA obligations.....	14
2.1.3 Subscriber Obligations	15
2.1.4 Relying party obligations.....	15
2.1.5 Repository Obligations.....	15
2.2 Liability.....	15
2.2.0 CA Liability	16
2.2.1 RA Liability.....	16
2.3 Financial responsibility	16
2.3.1 Indemnification by relying parties	16
2.3.2 Fiduciary relationships.....	16
2.3.3 Administrative processes.....	17
2.3.4 Client managed CA services	17
2.4 Interpretation and Enforcement.....	17
2.4.1 Governing Law.....	17
2.4.2 Serverability, survival, merger, notice	18
2.4.3 Dispute resolution procedures.....	18
2.5 Fees ¹⁹	
2.5.1 Certificate issuance or renewal fees	20
2.5.2 Certificate access fees	20
2.5.3 Revocation or status information access fees	20
2.5.4 Fees for other services such as policy information.....	20
2.5.5 Refund policy	20
2.6 Publication and repository.....	20
2.6.1 Publication of CA information.....	20
2.6.2 Frequency of publication	21

2.6.3	Access controls	21
2.6.4	Repositories	21
2.7	Compliance Audit.....	21
2.7.1	Frequency of entity compliance audit.....	21
2.7.2	Identity/qualifications of auditor.....	21
2.7.3	Auditor's relationship to audited party	21
2.7.4	Topics covered by audit	22
2.7.5	Actions taken as a result of deficiency	22
2.7.6	Communication of results.....	22
2.8	Confidentiality.....	22
2.8.1	Types of information to be kept confidential	22
2.8.2	Types of information not considered confidential	23
2.8.3	Disclosure of Certificate revocation/suspension information.....	23
2.8.4	Release to law enforcement officials	24
2.8.5	Release as part of civil discovery	24
2.8.6	Disclosure upon owner's request.....	24
2.8.7	Other information release circumstances	25
2.9	Intellectual Property rights	25
2.9.1	General provision	25
2.9.2	Copyright.....	25
3.	IDENTIFICATION AND AUTHENTICATION.....	26
3.1	Initial registration.....	26
3.1.1	Types of names.....	26
3.1.2	Need for names to be meaningful	26
3.1.3	Rules for interpreting various name forms	26
3.1.4	Uniqueness of names.....	27
3.1.5	Name claim dispute resolution procedure	27
3.1.6	Recognition, authentication and role of trademarks	27
3.1.7	Method to prove possession of private key	27
3.1.8	Authentication of organization identity	27
3.1.9	Authentication of individual identity	28
3.2	Routine Rekey.....	28
3.3	Rekey after Revocation.....	28
3.4	Revocation request.....	28
4.	OPERATIONAL REQUIREMENTS.....	29
4.1	Certificate Application	29
4.2	Certificate Issuance	29
4.2.1	Certificate issue process	29
4.3	Certificate acceptance	30
4.4	Certificate revocation.....	30
4.4.1	Circumstances for revocation.....	30
4.4.2	Who can request revocation	31
4.4.3	Procedure for revocation request.....	31
4.4.4	Revocation request grace period.....	31
4.4.5	Circumstances for suspension.....	31
4.4.6	Who can request suspension	31
4.4.7	Procedure for suspension request	31
4.4.8	Limits on suspension period	31
4.4.9	CRL issuance frequency	31
4.4.10	CRL checking requirements	32
4.4.11	On-Line revocation/status checking availability	32
4.4.12	On Line revocation checking requirements.....	32
4.4.13	Other forms of revocation advertisements available	32
4.4.14	Checking requirements for other forms of revocation advertisements	32
4.4.15	Special requirements for key compromise	32

4.5	Security Audit procedures	32
4.5.1	Types of events recorded	32
4.5.2	Frequency of processing log	33
4.5.3	Retention period for audit log	33
4.5.4	Protection of audit log	33
4.5.5	Audit log backup procedures	33
4.5.6	Audit collection system	33
4.5.7	Notification to event causing subject	33
4.5.8	Vulnerability assessments	33
4.6	Record Archival	34
4.6.1	Types of event recorded	34
4.6.2	Retention period for archive	34
4.6.3	Protection of archive	35
4.6.4	Archive backup procedures	35
4.6.5	Requirements for Time Stamping of records	35
4.6.6	Archive collection system	35
4.6.7	Procedures to obtain and verify archive information	35
4.7	Key changeover	35
4.8	Compromise and Disaster Recovery	36
4.8.1	Computing resources, software, and/or data are corrupted	36
4.8.2	Entity public key is revoked	36
4.8.3	Entity key is compromised	36
4.8.4	Secure facility after a natural or other type of disaster	36
4.9	CA termination	36
5.	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	38
5.1	Physical Controls	38
5.1.1	Site location and construction	38
5.1.2	Physical access	38
5.1.3	Power and air conditioning	38
5.1.4	Water exposures	38
5.1.5	Fire prevention and protection	38
5.1.6	Media storage	39
5.1.7	Waste disposal	39
5.1.8	Off-site backup	39
5.2	Procedural Controls	39
5.2.1	Trusted roles	39
5.2.2	Number of persons required per task	40
5.2.3	Identification and authentication for each role	40
5.3	Personnel Controls	40
5.3.1	Background, qualifications, experience, and clearance requirements	40
5.3.2	Background check procedures	40
5.3.3	Training requirements	40
5.3.4	Retraining frequency and requirements	41
5.3.5	Job rotation frequency and sequence	41
5.3.6	Sanctions for unauthorized actions	41
5.3.7	Contracting personnel requirements	41
5.3.8	Documentation supplied to personnel	41
6.	TECHNICAL SECURITY CONTROLS	42
6.1	Key Pair Generation and Installation	42
6.1.1	Key pair generation	42
6.1.2	Private key delivery to entity	42
6.1.3	Public key delivery to certificate issuer	42
6.1.4	CA public key delivery to users	42
6.1.5	Key sizes	42
6.1.6	Public key parameters generation	42

6.1.7	Parameter quality checking	42
6.1.8	Hardware/software key generation	42
6.1.9	Key usage purposes	42
6.2	Private Key Protection.....	43
6.2.1	Standards for cryptographic module	43
6.2.2	Private key (n out of m) multi-person control	43
6.2.3	Private key escrow	43
6.2.4	Private key backup	43
6.2.5	Private key archival	43
6.2.6	Private key entry into cryptographic module	43
6.2.7	Method of activating private key.....	43
6.2.8	Method of deactivating private key	43
6.2.9	Method of destroying private key	43
6.3	Other Aspects of Key Pair Management.....	44
6.3.1	Public key archival.....	44
6.3.2	Usage periods for the public and private keys	44
6.4	Activation Data	44
6.4.1	Activation data generation and installation	44
6.4.2	Activation data protection.....	44
6.4.3	Other aspects of activation data	44
6.5	Computer Security Controls.....	44
6.5.1	Specific computer security technical requirements.....	44
6.5.2	Computer security rating.....	44
6.6	Life Cycle Technical Controls.....	44
6.6.1	System development controls	44
6.6.2	Security management controls.....	45
6.6.3	Life cycle security ratings	45
6.7	Network Security Controls	45
6.8	Cryptographic Module Engineering Controls	45
7.	CERTIFICATE AND CRL PROFILES.....	46
7.1	Certificate Profile	46
7.1.1	Version number(s)	46
7.1.2	Certificate extensions.....	46
7.1.3	Algorithm object identifiers.....	46
7.1.4	Name forms	46
7.1.5	Name constraints	47
7.1.6	Certificate policy Object Identifier.....	47
7.1.7	Usage of Policy Constraints extension	47
7.1.8	Policy qualifiers syntax and semantics	47
7.1.9	Processing semantics for the critical certificate policy extension	47
7.2	CRL Profile.....	47
7.2.1	Version number(s)	47
7.2.2	CRL and CRL entry extensions	47
8.	SPECIFICATION ADMINISTRATION.....	48
8.1	Specification change procedures	48
8.1.1	Initial publication.....	48
8.1.2	Change.....	48
8.2	Publication and notification policies	49
8.3	CPS approval procedures	49
9.	Appendix A - Glossary.....	50
	Appendix B - Organisation Proof Of Identity form ¾ User Details.....	68
	Proof Of Identity form — Organisation	70

SDPL RCA CPS₍₁₎

**SECURITY DOMAIN PTY LIMITED
ROOT CERTIFICATION
AUTHORITY**

CERTIFICATE POLICY STATEMENT

SCHEME:	SDPL
ACCREDITATION	-
TYPE:	RCA
GRADE:	-
STATUS:	Released

1. INTRODUCTION

1.1 Overview

This CPS₍₁₎ has been written expressly to support the use of Certificates created under the Certificates On-Line infrastructure (“SDPL 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.

Certificates On-Line endorses three types of Certificate aimed at certifying Individuals, Organisations and Employees.

Security Domain provides two types of key pairs to End Users:

- authentication key pairs; and,
- confidentiality key pairs.

Each key pair consists of a private and a public key.

An authentication key pair is used for authentication, integrity and non-repudiation. The private key is used to digitally sign a message and the public key is used to verify a digital signature.

A confidentiality key pair is used to protect the confidentiality of a message. The public key is used to encrypt the contents of a message and the private key is used to decrypt the message.

1.1.1 Standards

This CPS₍₁₎ is referred to as the “Security Domain Pty Limited RCA CPS₍₁₎”.

This CPS₍₁₎ is based on the IETF PKIX 4 Draft, however in some instances the document does not allow adequate definition.

Where the standard does provide for sufficient definition this CPS₍₁₎ will differ from the standard in so far as it is necessary for clarity only.

1.1.2 Certificate types issued

The SDPL RCA shall issue the following types of Certificates:

1. subordinate Certification Authority (CA) Certificates:
 - Demonstration CA;
 - User CA;
 - Outsourced User CA;

2. such other Certificates as might be approved by the Security Domain Pty Limited Policy Approval Authority.

1.1.3 Definitions

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.

1.2 Identification

This CPS₍₁₎ is referred to as the "Security Domain Pty Limited RCA CPS₍₁₎".

1.2.1 X500 Object Identifier hierarchy

The authority for all objects identified under this Policy originates from the SDPL RCA Infrastructure (PKI).

Specified elements under this Public Key Infrastructure (PKI) have been assigned an X.500 Object Identifier (OID).

1.2.2 SDPL RCA OID

The X.500 Object Identifier (OID) for the SDPL RCA is:

1,2,36,82074575,1

1.2.3 SDPL RCA CPS₍₁₎ OID

The OID for this policy is:

1,2,36,82074575,1,1,1,0

1.3 Community and Applicability

This policy is applicable to the:

1. subordinate Certification Authority (CA) 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/>

- Demonstration CA;
 - User CA;
 - Outsourced User CA;
2. such other Certificates as might be approved by the Security Domain Pty Limited Policy Approval Authority.

This section provides a description of each of these elements, including their respective obligations, roles and responsibilities.

1.3.0 Policy Authorities

Two Policy Approval Authorities are relevant to this CPS₍₁₎, they are:

Security Domain Pty Limited Policy Approval Authority (SDPL PAA), which sets out the over arching operational doctrine for the SDPL PKI.

Policy Creation Authorities (PCA) which are responsible for the creation of policy unique to the operation of a particular CA. For the purpose of this CPS₍₁₎ the PCA function shall be carried out directly by the SDPL PAA.

The contact details for the SDPL PAA are:

Name:	Security Domain Pty Limited
Contact:	Policy Approval Authority
Title:	General Manager - Certificates On-Line
ACN:	82074575
Trading as:	Security Domain
OID:	N/a
Postal Address:	Level 5, 1 James Place, North Sydney NSW 2060 Australia
Phone:	+61 2 9409 0300
Fax:	+61 2 9409 0301
E-Mail Address:	info@secdom.com.au

1.3.0.1 SDPL PAA Functions

The SDPL Policy Approval Authority (PAA) has the following functions:

1. to approve CPS₍₁₎ within the hierarchy;
2. approve the establishment of Policy Creation Authorities (PCA);
3. administer subordinate policy infrastructure to maintain the total integrity of the PKI.

1.3.1 Certification authorities

1.3.1.1 SDPL Root CA

The Root CA in operation is the Security Domain Pty Limited RCA (SDPL RCA). The registered address of which is:

Security Domain Pty Limited
Level 5, Number 1 James Place
North Sydney NSW 2060

1.3.1.2 SDPL RCA Functions

The SDPL RCA has the following functions, to:

1. generate its own keys and issue a self signed Certificate, publishing the public key;
2. certify the public key of a subordinate CA when requested to do so;
3. operate in accordance with documented operational practice.

1.3.1.3 Contact Details

The contact details for the SDPL RCA are:

Name:	Security Domain Pty Limited Root CA
ACN:	82074575
Trading as:	Security Domain RCA
OID:	1.2.36.82074575.1
Postal Address:	Level 5, 1 James Place, North Sydney NSW 2060, Australia
Phone:	+61 2 9409 0300
Fax:	+61 2 9409 0301
Domain Name:	www.secdom.com.au
E-Mail Address:	info@secdom.com.au
Contact:	General Manager – Certificates On-Line

1.3.2 Registration authorities

Not applicable to this CPS₍₁₎ as the RCA is responsible for Proof Of Identity (POI) and the collection of Certificate information for subordinate CAs.

1.3.3 End entities

Not applicable to this CPS₍₁₎.

1.3.4 Applicability

Certificates issued under this CPS₍₁₎ are limited to:

1. subordinate CA Certificates;
2. such other Certificates as might be approved by the SDPL PAA.

Certificates issued under this CPS₍₁₎ can be used to request routine rekey.

1.4 Contact Details

1.4.1 Specification administration organization

This CPS₍₁₎ 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 Person determining CPS suitability for the policy

See 1.4.2 *Contact person*.

2. GENERAL PROVISIONS

This section covers all of the legal requirements of the SDPL RCA to entities relying on Certificates issued under its hierarchy. These requirements include:

- obligations;
- liability;
- financial responsibility;
- interpretation and enforcement;
- fees;
- publication and repository;
- confidentiality;
- intellectual property rights.

2.1 Obligations

This section covers the obligations of SDPL and the SDPL RCA to all entities relying on Certificates issued under the SDPL RCA hierarchy.

2.1.0 SDPL Obligations

SDPL shall provide a secure PKI that enables the operation of keys and certificates using public key cryptographic methods. The SDPL RCA shall be the highest point of trust within the infrastructure and there shall be two types of Certification Authority (CA), these shall be:

1. SDPL CA;
2. Client CAs.

2.1.0.1 PAA Obligations

The SDPL PAA has the right and will at all times have the right to alter or amend this CPS₍₁₎ and will publish on its web page the amended CPS₍₁₎ which will specify the time at which the new CPS₍₁₎ will apply.

2.1.1 CA Obligations

The SDPL Root CA will provide Certificates to a subordinate CA on receipt of a properly formatted certification request.

The Certificate carries with it a 'policy qualifier' which is used to bring out the major points of the SDPL RCA CPS₍₁₎.

The SDPL RCA discharges its obligations under this CPS₍₁₎ by:

1. providing and maintaining 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₍₁₎;
 - 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₍₁₎ 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. making reasonable inquiry to determine the validity of compromises and suspected compromises of private keys at any subordinate level it deems warranted in its chain of trust;
10. revoking Certificates on receipt of authenticated digitally signed revocation requests, or when its inquiries into the compromise or suspected compromise of a private key have established the validity of a revocation request;
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.

2.1.2 RA obligations

Not applicable to this CPS₍₁₎.

2.1.3 Subscriber Obligations

Not applicable to this CPS⁽¹⁾.

2.1.4 Relying party obligations

Not applicable to this CPS⁽¹⁾.

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 section 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.

2.2.0.1 PAA liability

The SDPL PAA shall not be held liable for any CPS₍₁₎ created, modified or used within the SDPL Hierarchy.

2.2.0 CA Liability

The SDPL RCA has certified the SDPL CA to issue keys and Certificates that comply with SDPL Certificate requirements.

In no event is the Root CA liable for any direct, indirect, special, economic or consequential loss or damage or loss of revenue, profits, goodwill, bargain, opportunities, loss or corruption of data or loss of anticipated savings arising from use of keys or a Certificate whether caused by negligence or otherwise and whether or not the RCA was aware or should have been aware of the possibility of such loss or damage.

To the fullest extent permitted at law under this policy the RCA accepts no liability and all parties using any private keys of Certificates or relying upon any information specified in any Certificates (Especially any public keys identified in any Certificates) issued or generated under or in connection with or relating to this CPS₍₁₎ accept that in so using or relying upon the Private key or Certificate that the RCA has no liability

To the fullest extent permitted at law and in equity and by statute all implied warranties under any federal or state legislation are excluded.

The SDPL RCA is not liable for the operation of Security Domain CA or any consequence of malfeasance, tort or contractual breach arising from the operation thereto.

2.2.1 RA Liability

Not applicable to this CPS₍₁₎.

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 in accordance with this CPS₍₁₎ does not make Security Domain Pty Limited or the SDPL RCA an agent, fiduciary, trustee, or other representative of the certificate holders or relying parties.

2.3.3 Administrative processes

Security Domain Pty Limited is a wholly owned subsidiary of Baltimore. Baltimore is a publicly listed company on the London Stock Exchange (LSE).

Security Domain has undergone a review by the Australian Commonwealth Government and has been included in the Government Endorsed Supplier scheme.

Government Endorsed Supplier status includes production and verification of financial viability.

2.3.4 Client managed CA services

Security Domain may request customers who apply to manage CA services within the SDPL PKI to provide supporting documentation during initial registration. Customers are to 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 policy is governed by the laws in force in New South Wales Australia. In addition to this, the policy is reliant upon a contract structure from the SDPL RCA to the subordinate SDPL CA.

Furthermore, all parties using or relying upon this CPS₍₁₎ submit to the non exclusive jurisdiction of the Courts of New South Wales and all Courts of Appeal from them.

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.

2.4.1.2 Subordinate contract structure

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 CA 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 Serverability, survival, merger, notice

2.4.2.1 Severability

In the event that any one or more of the provisions of this CPS₍₁₎ 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₍₁₎ 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₍₁₎.

2.4.2.2 Survival (Continuing obligations)

This CPS₍₁₎ shall be binding upon, and inure to the benefit of all parties hereto. The rights and obligations detailed in this CPS₍₁₎ 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₍₁₎ applies is compromised or the expiration date of a certificate to which this CPS₍₁₎ 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

Any amendments to this policy or the RCA hash will be updated on the following web site:

www.secdom.com.au

2.4.3 Dispute resolution procedures

2.4.3.1 Hierarchy of Certificate policy

In the event that a dispute arises between parties under the SDPL hierarchy the following precedence will apply:

1. where the subject of the dispute is covered by a contract e.g. between the RCA and a CA then the contract shall prevail;
2. where the subject of the dispute is covered wholly within this CPS₍₁₎ e.g. between the SDPL RCA and a subordinate CA then this policy shall prevail.

This policy does not support third party reliance, e.g. between an SDPL Certificate and a non-SDPL Certificate.

2.4.3.2 Process

If a dispute arises in connection with this CPS₍₁₎, 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

Fees are payable in respect to the issue, renewal or revocation of CA Certificates.

No fee is levied for access to this CPS₍₁₎ via the Internet. Printed copies of this policy are available from the SDPL PAA for a fee of \$AUD5.00 plus postage and packaging.

2.5.1 Certificate issuance or renewal fees

Fees are payable by CAs in respect to the issue or renewal of their Certificates and such fees shall be advised on application.

2.5.2 Certificate access fees

Fees are payable by CAs in respect to access to SDPL X.500 Directory services for Certificate downloading and such fees shall be advised on application.

2.5.3 Revocation or status information access fees

Fees are payable by CAs in respect to access to SDPL X.500 Directory services for Certificate revocation or status information and such fees shall be advised on application.

2.5.4 Fees for other services such as policy information

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

Fees are payable by CAs in respect to the revocation or suspension of Certificates and such fees shall be advised on application.

2.5.5 Refund policy

A refund policy may apply to nominated fees. Refund policy shall be advised on application.

2.6 Publication and repository

2.6.1 Publication of CA information

This Certificate policy and the Root CA Hash will be published on the following web sites:

www.secdom.com.au

www.baltimore.com

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₍₁₎ and relevant CPS₍₂₎ are published promptly.

2.6.3 Access controls

There are no access controls on the reading of this CPS₍₁₎ or of relevant CPS₍₂₎ 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 all public keys, Certificates and user information shall be the SDPL X.500 Directory. The SDPL X.500 Directory shall be accessed via:

www.secdom.com.au

www.baltimore.com

2.7 Compliance Audit

2.7.1 Frequency of entity compliance audit

The issuer of this policy has completed an evaluation of the technology and supporting infrastructure. The evaluation criteria appear in section 2.7.4 *Topics covered by audit*.

2.7.2 Identity/qualifications of auditor

Any firm or person contracted to perform a security audit on the SDPL RCA 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 shall consist of:

1. physical security;
2. documentation and process;
3. vetting of operations personnel;
4. technology;
5. privacy, including compliance with Commonwealth Information Privacy Principles;
6. financial viability and industry development.

2.7.5 Actions taken as a result of deficiency

Audit reports are submitted to General Manager – Certificates On-Line.

When irregularities are found, General Manager – Certificates On-Line shall promptly implement 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 for Cryptography Policy

This policy conforms to the OECD Guidelines on the use of public key infrastructure.

Application of Commonwealth Information Privacy Principles

The SDPL RCA shall comply with the Commonwealth Information Privacy Principles.

Tax File Number legislation

Not Applicable.

Confidential information

All information collected or held by SDPL shall only be used in support of the operations of this public key infrastructure, or in support of a compliant transaction.

Information collected in support of this CPS₍₁₎ will fall into two categories;

1. Proof Of Identity information, e.g. Registration Records;
2. Certificate information, e.g. information used to populate a field in an X.509 Certificate.

2.8.1.2 Registration information

This CPS₍₁₎ requires that identification documentation to a value of 150 points be produced to support the issue of a SDPL RCA and subordinate CA Certificate.

Proof Of Identity information is collected at the time that an organisation applies for the issue of public keys and CA Certificates (Registration Record).

Registration records are considered to be confidential information.

2.8.1.3 Certificate information

At the time a Registration record is created, certain information will be collected. Some of this collected information will appear in an X.509 V3 Certificate.

Information embodied in a Certificate held as part of the registration record is not considered to be confidential. All other information concerning the registration record will be considered confidential. This provision does not operate to prevent publication of the Certificate information.

2.8.2 Types of information not considered confidential**2.8.2.1 Certificate information**

Certificate information is not confidential and is deemed to be public knowledge where:

1. the Certificate is used in its intended fashion;
2. the information appears in a public directory.

2.8.3 Disclosure of Certificate revocation/suspension information

Certificate suspension is not supported.

2.8.3.1 Disclosure of Certificate suspension information

Certificate suspension is not supported.

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 principal, no document or record belonging to the SDPL RCA shall be released to law enforcement agencies or officials except where:

1. a properly constituted warrant is produced;
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 the SDPL RCA shall be released to any person except where:

1. a properly constituted instrument that has emanated from a court having jurisdiction or an authority having legal jurisdiction (e.g. the Australian Securities Investment Commission) requiring production of the information is produced; and
2. the person requiring production is a person authorised to do so.

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.

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

SDPL warrants that it is in possession of, or holds licences for the use of hardware and software in support of this CPS₍₁₎.

SDPL further warrants that operational use of this CPS₍₁₎ does not infringe any copyright enforceable in Australia of any third party.

SDPL excludes all liability for breach of any other intellectual property right.

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.

The use of the PKIX IETF Draft 4 Guideline for drafting CPS₍₁₎ is acknowledged.

2.9.1.2 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.

2.9.1.3 Distinguished names

Intellectual property rights in distinguished names shall vest in the assigning party unless otherwise specified in contract.

2.9.2 Copyright

2.9.2.1 General

The intellectual property in this CPS₍₁₎ is the exclusive property of SDPL.

2.9.2.2 in OID

Copyright in the Object Identifiers (OID) for the SDPL public key infrastructure vest solely in the SDPL.

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 this policy.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial registration

The application for a CA shall constitute three functions:

1. collection of Certificate information;
2. Proof Of Identity;
3. completion of an RCA-CA agreement.

A recommended format for the collection of Proof Of Identity for a CA appears at Appendix B to this CPS₍₁₎.

3.1.1 Types of names

All Distinguished Names shall comply with the X.520 Certificate standard.

The Distinguished Name for the SDPL RCA shall be:

Common Name:	Root CA
Organisation:	Security Domain Pty Limited
Organisational Unit:	Not Applicable
Locality:	Level 5, 1 James Place, North Sydney 2060
State or Province:	NSW Australia

3.1.2 Need for names to be meaningful

Distinguished Names for SDPL RCA subordinate Certificates must be meaningful. Pseudonymous names may be used in the common name component of a distinguished name where requested by a CA, provided the CA can satisfactorily establish their right to use the pseudonym.

Pseudonymous names which may cause offence shall not be permitted.

3.1.3 Rules for interpreting various name forms

The normal operation of the Certificate generation requires the insertion of the Organisation name and department as part of the Distinguished Name.

The Certificate being generated here is an RCA Certificate, this Certificate does not require a department identifier.

The following changes are to be made to the Distinguished Name:

Department name	Not Applicable
-----------------	----------------

3.1.4 Uniqueness of names

The Distinguished Name shall be unambiguous and unique.

3.1.5 Name claim dispute resolution procedure

Any dispute regarding a Distinguished Name will be 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 a CA, the RCA must satisfy itself that the CA does in fact possess the private keys that correspond to the public keys received from the CA.

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

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

1. the RCA checking 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 warranty from the organisation and a statutory declaration from each of the principals that the CA is the true owner of the key pairs.

If any doubt exists, the RCA is not to certify the keys. If the subordinate CA'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 recorded;
2. the application may be progressed using key pairs generated by the RCA.

3.1.8 Authentication of organization identity

The RCA must satisfy itself as to the identity of the CA. This process requires the completion of an organisational Proof of Identity (POI) form as attached at Appendix B.

3.1.9 Authentication of individual identity

Not applicable for CA certificates.

3.2 Routine Rekey

CA keys and Certificates shall remain valid for a period of seven (7) years from the date of establishment.

Routine rekey may be completed on line provided that:

1. the keys and Certificates are valid (e.g. not expired) at the time the routine rekey falls due;
2. the CA's identification details as contained in the Proof of Identity records have not changed;
3. the CA has not been listed as a compromised CA;
4. the CA's keys have not been listed as compromised keys;
5. the renewal request is digitally signed:
 - by a valid key pair and Certificate;
 - under this CPS₍₁₎.

3.3 Rekey after Revocation

After revocation of a CA's keys and Certificates rekey shall be by way of a new application.

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 this CPS₍₁₎ constitutes a valid and enforceable revocation request.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The RCA key and Certificate shall be applied for by the unanimous resolution of the SDPL PAA.

An application by a third party to operate a subordinate CA shall 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 a CA service.

4.2 Certificate Issuance

The RCA key and Certificate shall be generated and issued promptly on receipt of an authorised application from the SDPL PAA.

Keys and a Certificate shall be issued promptly to a subordinate CA only after completion of a valid registration process. The registration process shall include the:

- clear identification of the CA to the prescribed level;
- execution of required contractual documents;
- submission of required policy and operational documents, including but not limited to this CPS₍₁₎, a relevant CPS₍₂₎ and CONOPS.

4.2.1 Certificate issue process

In order for a CA to be issued with a Certificate, it must first be identified by the RCA to meet the authentication requirements of this CPS₍₁₎.

Subordinate CAs deliver a Certificate request file to the RCA. The RCA creates a CA Certificate from the request file then delivers the generated and signed Certificate to the CA.

The files are normally exchanged using manual delivery, but may be exchanged electronically where appropriate procedures, controls and or mechanisms are in place to protect the integrity of the request.

The CA is then able to use their CA software to certify subordinate entities in the hierarchy.

4.3 Certificate acceptance

A CA's receipt of a Certificate, and its subsequent use of its keys and Certificate, constitutes Certificate acceptance.

The use of the Certificate also constitutes acceptance of the terms of this policy.

4.4 Certificate revocation

4.4.1 Circumstances for revocation

The RCA's or a subordinate CA's Certificate is revoked in the event of:

1. the theft, loss, disclosure, modification, or other compromise or suspected compromise of private key(s)
2. the deliberate misuse by a subordinate CA 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₎;
3. the RCA or subordinate CA ceases operations;
4. the 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;
5. material Certificate information becoming inaccurate, for example in the event of a subordinate CA changing its name;
6. a properly formatted request being received from the SDPL PAA (for the SDPL RCA) or from the subordinate CA;
7. a validated request being received from an authorised third party, for example a court order;
8. for subordinate CAs, the RCA Certificate being revoked;
9. it becoming known or there being reason to believe a subordinate CA 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. the SDPL PAA, for the RCA Certificates;
2. the RCA, for subordinate CA Certificates;
3. a subordinate CA, for its own Certificates;
4. an authorised third party, for example a Court of New South Wales.

4.4.3 Procedure for revocation request

RCA revocation can only be initiated after the SDPL PAA have met and a resolution has been made to revoke the RCA.

CA revocation requires the written approval of General Manager - Certificates On-Line.

4.4.4 Revocation request grace period

Revocation requests are to be:

1. verified on receipt;
2. actioned promptly.

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

All CAs should check the SDPL X.500 Directory to satisfy themselves as to the currency and validity of the RCA Certificate under which their CA Certificates have been signed.

4.4.11 On-Line revocation/status checking availability

SDPL provides an on line mechanism for verifying the status of Certificates issued under this hierarchy through:

1. X.500 Directory;
2. publication of the RCA Hash.

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

The RCA supports only the SDPL X.500 Directory for CRLs.

4.4.14 Checking requirements for other forms of revocation advertisements

The RCA supports only the SDPL X.500 Directory for CRLs.

4.4.15 Special requirements for 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 is obliged under contract to maintain adequate records and maintain archives of information pertaining to the operation of the public key infrastructure.

4.5.1 Types of events recorded

Nominally records to be kept include:

1. registration records;
2. key generation requests;
3. Certificate generation requests;
4. Certificate issuance records, including CRLs;
5. audit records including security related events.

4.5.2 Frequency of processing log

Processing of logs shall be undertaken on the following frequency:

Annual, monthly weekly and daily.

4.5.3 Retention period for audit log

The audit log shall be retained for a minimum period of seven years or such other time (not exceeding ten years) as required to meet the Australian archives requirements. At the completion of that term, the audit log is transferred to Australian Archives for which a fee shall be charged.

4.5.4 Protection of audit log

The audit log shall be encrypted using a specifically generated key and Certificate for the purpose.

4.5.5 Audit log backup procedures

Each element of the SDPL hierarchy shall establish and maintain a backup procedure for audit logs.

4.5.6 Audit collection system

The RCA audit collection system shall be a combination of automated and manual processes performed by the operating system, the RCA software, and by operational personnel.

4.5.7 Notification to event causing subject

RCA operations personnel notify the 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 CAs and RAs.

4.6 Record Archival

The SDPL RCA shall maintain an archive of relevant records described in this policy.

4.6.1 Types of event recorded

The following information shall be archived by the SDPL RCA:

1. audit logs of the SDPL RCA;
2. Certificate request information;
3. Certificates, including CRLs generated;
4. complete back up records;
5. copies of email logs;
6. formal correspondence;

4.6.2 Retention period for archive

4.6.2.1 Secure maintenance of keys

In accordance with OECD Guidelines for Cryptography Policy only Confidentiality keys are archived. The period for archiving confidentiality keys is a minimum period of seven years from the date of generation or such other time (not exceeding ten years) as required to meet the Australian archives requirements. At the completion of that term, the Confidentiality keys are transferred to Australian Archives for which a fee is charged.

The confidentiality keys shall be archived securely on a CD ROM.

4.6.2.2 Secure maintenance of Certificate

RCA and subordinate CA Certificates shall be archived for a minimum period of seven years from the date of generation, unless another period is specifically required.

The Certificates shall be archived securely on a CD ROM.

4.6.2.3 Term of archive maintenance

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

The audit logs shall be archived securely on a CD ROM.

4.6.3 Protection of archive

Archive media shall be 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

Archive back-up procedures have been established to ensure complete restoration of current service or verification.

4.6.5 Requirements for Time Stamping of records

Trusted third party time stamping is not supported under this policy.

4.6.6 Archive collection system

Archiving shall be done by the SDPL internal operation staff delegated with the responsibility for doing so.

4.6.7 Procedures to obtain and verify archive information

The integrity of the archives should be verified:

1. annually at the time of the programmed security audit;
2. at any time when a full security audit is required;
3. at the time that the archive has been prepared.

4.7 Key changeover

RCA Certificates have a seven year validity period. The SDPL RCA will publish notice of its intention to effect a key change twelve months prior to the expiry of the existing keys and Certificates.

On the Seventh anniversary of the Date of Establishment the RCA shall generate a set of X.509 keys and self certify those keys within:

- a) the terms of this CPS₍₁₎;
- b) the prevailing X.509 standard, currently Version 3 (23/12/98);
- c) the prevailing certificate profile.

4.8 Compromise and Disaster Recovery

The RCA and the SDPL hierarchy shall maintain detailed documentation covering:

1. Contingency Planning and Disaster Recovery;
2. Configuration Baseline of the Root hierarchy;
3. OID hierarchies;
4. back-up, archiving and offsite storage.

These plans will be made available to those persons responsible for conducting a security audit.

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

The SDPL RCA 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

The RCA and each subordinate CA has established a key and user compromise plan that addresses the actions to be taken in the event that the SDPL RCA or a subordinate CA public key is revoked.

4.8.3 Entity key is compromised

The RCA and each subordinate CA 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

Backup, archive and offsite storage shall be managed in accordance with the Configuration Baseline of the RCA and its associated back-up, archiving and offsite storage plan.

4.9 CA termination

In the event that it becomes necessary to terminate the SDPL RCA or a subordinate 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.

In the case of a programmed termination of a subordinate CA a minimum of three month's notification shall be given to approved RAs of the proposed shut down. Approved RAs shall be responsible for advising all End Users.

In the event of an emergency shut down of a CA, e.g. in the case that the CA private key is compromised the CA will give as much notice as is practical and reasonable under the prevailing circumstances.

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 shall be in a secure office environment at Level 5, 1 James Place, North Sydney NSW Australia.

The RCA shall be operated within a secure physical environment within the office area that shall meet the standards required by ACSI 33 CR2.

5.1.2 Physical access

SDPL shall permit 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 shall be kept to a minimum and a log shall be maintained of all accesses.

5.1.3 Power and air conditioning

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

The area shall have an air conditioning system to control the heat and humidity that shall be independent of the building air conditioning system.

5.1.4 Water exposures

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

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

5.1.5 Fire prevention and protection

Suitable fire extinguishers shall be maintained in the RCA secure operating area, to guard against the possibility of fire.

5.1.6 Media storage

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

5.1.7 Waste disposal

Paper documents and magnetic media containing the RCA private key or commercially sensitive or confidential information shall be 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 shall be used for the storage and retention of backup software and data.

The off site storage:

1. shall be available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data;
2. shall have 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 an RCA service workstation shall be shared by multiple roles and individuals. Oversight may be in the form of a person who shall be not directly involved in issuing certificates examining system records or audit logs to ensure that other persons have acted within the realms of their responsibilities and within the stated security policy.

This shall be accomplished by creating separate roles and accounts on the RCA service workstation, each of which shall have a limited amount of capability. This method shall allow a system of "checks and balances" to occur among the various roles. At a minimum, the following roles shall be established:

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

5.2.2 Number of persons required per task

Separate individuals shall fill each of the three roles described above. This shall provide the maximum security and shall afford 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 shall 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 shall 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 shall undergo a formal vetting process, designated "Position of Trust".

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The recruitment and selection practices for RCA services personnel shall take into account the background, qualifications, experience and clearance requirements of each position, which shall be compared against the profiles of potential candidates.

5.3.2 Background check procedures

Background checks shall be 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 RCA services personnel staff shall be trained in:

1. basic PKI concepts;
2. the use and operation of the RCA software;
3. documented RCA procedures;
4. computer security awareness and procedures;
5. how to explain to CA certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
6. the meaning and effect of this CPS₍₁₎, and a relevant CPS₍₂₎.

5.3.4 Retraining frequency and requirements

RCA services personnel staff shall receive a security briefing update at least once a year.

Training in the use and operation of the RCA software shall be provided when new versions of the software are installed.

Remedial training shall be completed when recommended by audit comments.

5.3.5 Job rotation frequency and sequence

The RCA may implement formal job rotation practices (e.g. through formal reliefs). Where formal job rotation is not implemented, cross-training activities shall be conducted to ensure operations continuity.

5.3.6 Sanctions for unauthorized actions

Unauthorised actions by RCA services personnel staff shall be submitted to appropriate authorities including, but not limited to, the Security Administrator.

5.3.7 Contracting personnel requirements

RCA services personnel may be contractors who shall be appointed in writing and given written notification of the terms and conditions of their position. They shall be normally assigned full-time to their responsibilities.

5.3.8 Documentation supplied to personnel

RCA services personnel shall have access to all relevant:

1. hardware and software documentation;
2. policy documents, including this CPS₍₁₎;
3. operational practice and procedural documents, including a relevant CPS₍₂₎.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

RCA key pairs shall be generated and installed by the RCA.

6.1.2 Private key delivery to entity

The self-generated RCA private keys do not require delivery.

6.1.3 Public key delivery to certificate issuer

The self-generated RCA public keys do not require delivery.

6.1.4 CA public key delivery to users

The self-generated RCA public keys do not require delivery.

6.1.5 Key sizes

The RCA key lengths shall be determined by a relevant Certificate profile. They shall typically be a minimum of 2048 bits.

6.1.6 Public key parameters generation

The parameters used to create public keys shall be generated by the RCA.

6.1.7 Parameter quality checking

The quality of public key parameters shall be automatically checked by the RCA software.

6.1.8 Hardware/software key generation

RCA key generation shall be performed in hardware or software as prescribed by security policy.

6.1.9 Key usage purposes

Keys may be used for the purposes and in the manner described in section 1.3.4 *Applicability*.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

Cryptographic modules that may be in use from time to time as part of the operations of the RCA shall comply with industry standards.

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

Private keys shall not be under n out of m multi-person control.

6.2.3 Private key escrow

Private key escrow shall be not supported.

6.2.4 Private key backup

The RCA private key shall be stored in an encrypted database, which shall be backed up under further encryption with backup copies maintained on site and in secure off site storage.

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

Where a cryptographic module is used, the private key shall 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 shall be activated by the RCA software, following the successful completion of a login process that requests and validates an authorised user access control mechanism.

6.2.8 Method of deactivating private key

Private keys shall be de-activated when the RCA software application is terminated.

6.2.9 Method of destroying private key

The RCA software shall destroy private keys in memory by overwriting them with zeros when the software shuts down.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The RCA shall archive its public key.

6.3.2 Usage periods for the public and private keys

The usage period for the RCA private and public key shall be ten years.

6.4 Activation Data

6.4.1 Activation data generation and installation

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

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

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

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The RCA has established a System Security Plan that incorporates computer security technical requirements for the operation of the RCA.

6.5.2 Computer security rating

The RCA has established a System Security Plan that incorporates computer security ratings for the operation of the RCA.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

RCA operational software shall be developed in a controlled environment employing appropriate quality controls.

6.6.2 Security management controls

System security management shall be 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

The RCA has established a Protective Security Risk Review that identifies and addresses all high or significant life cycle security threats.

6.7 Network Security Controls

The RCA has established a Protective Security Risk Review that identifies and addresses all high or significant network security threats.

6.8 Cryptographic Module Engineering Controls

The RCA has established a 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 RCA supports and uses X.509 Version 3 certificates, which contain v.3 in the version field.

7.1.2 Certificate extensions

The RCA supports and uses X.509 Version 3 certificate extensions.

7.1.3 Algorithm object identifiers

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

The following hashing/digest algorithms shall be supported:

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

The following padding algorithms shall be supported:

1. ISO 9796;
2. PKCS#1.

The following encryption algorithms shall be supported:

1. RSA;
2. DES.

The use of multiple algorithms within the same hierarchy shall be supported.

7.1.4 Name forms

Certificates issued by the RCA 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 shall be not supported. Pseudonymous names that may cause offence shall be not permitted.

7.1.6 Certificate policy Object Identifier

The OID of this CPS₍₁₎ shall be carried in the standard extension field of X.509 certificates and is published in this CPS₍₁₎.

7.1.7 Usage of Policy Constraints extension

The RCA shall support the use of the Policy Constraints extension.

7.1.8 Policy qualifiers syntax and semantics

The RCA shall support the use of syntax and semantics policy qualifiers.

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 RCA supports and uses X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

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

8. SPECIFICATION ADMINISTRATION

SDPL operates a PAA which has the responsibility for setting CPS₍₁₎ direction for the over all public key infrastructure. Contact details for the PAA appear elsewhere in this policy.

Normally subordinate to a PAA is a Policy Creation Authority (PCA), which is vested in a CA or equivalent, in the case of this CPS₍₁₎, the PAA and PCA functions are vested in the same authority, the SDPL PAA.

Each CPS₍₁₎ used within the SDPL PKI has been allocated an OID. The OID provides a unique identification for each CPS₍₁₎ that represents a policy version number.

8.1 Specification change procedures

8.1.1 Initial publication

The responsible authority for changes to this CPS₍₁₎ and subordinate CA CPS₍₁₎ is the SDPL PCA. The SDPL RCA will request formal endorsement and allocation of an OID.

After the OID has been granted, the SDPL RCA will publish, on the SDPL World Wide Web page, the SDPL RCA CPS₍₁₎. SDPL RCA will then be responsible for advising all subordinate elements of the CPS₍₁₎ and its applicability.

8.1.2 Change

Two forms of policy change are contemplated:

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

In the event that this CPS₍₁₎ requires re-issue, then the change process employed will be as for initial publication above.

Where a policy change is required the OID of the CPS₍₁₎ will remain in force, however a new version number will be allocated by the PCA on endorsement of the CPS₍₁₎ by the SDPL PAA.

Following approval, the SDPL PAA will facilitate publication of the new CPS₍₁₎.

8.2 Publication and notification policies

The new SDPL RCA CPS₍₁₎ shall be published on the SDPL World Wide Web page. Subordinate entities will be notified of changes to the CPS₍₁₎ as and when they occur. A minimum notice period of one week will be in force for subordinate entity infrastructure.

8.3 CPS approval procedures

The SDPL RCA CPS₍₁₎ must be endorsed by the SDPL PAA. A document setting out the functions of the SDPL PAA will be made available to the SDPL PCA, the document will also be 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	<p>A security assessment in respect of a person that contains:</p> <p>(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</p> <p>(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.</p>
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.

Term or Acronym	Explanatory notes
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
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.

Term or Acronym	Explanatory notes
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.
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.

Term or Acronym	Explanatory notes
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.
CASP	A Certification Authority Service Provider.
CBC	Cipher Block Chaining
Certificate ³	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.
Certificate Revocation List (CRL)	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: <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.

³ Definition from SAA MP75 (Standards Australia).

Term or Acronym	Explanatory notes
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. ⁴</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.

⁴ Ibid.

Term or Acronym	Explanatory notes
Communications Security (COMSEC)	<p>All measures applied to the protection of telecommunications from unauthorised interception and exploitation. Communications Security includes:</p> <p>(a) Crypto security - That component of communications security which results from the provision of technically sound cryptosystems and their proper use:</p> <p>(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</p> <p>(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).</p>
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*	<p>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.</p> <p>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.</p>
Cryptographic equipment*	Equipment in which cryptographic functions (e.g. encipherment, authentication, key generation) are performed.

Term or Acronym	Explanatory notes
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.
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 ⁵	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.

⁵ Ibid.

Term or Acronym	Explanatory notes
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.
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.

Term or Acronym	Explanatory notes
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. NOTES:</p> <ul style="list-style-type: none"> - 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. - 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.
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>

Term or Acronym	Explanatory notes
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.
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

Term or Acronym	Explanatory notes
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.
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.

Term or Acronym	Explanatory notes
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*	<p>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.</p> <p>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.</p>
Private key*	<p>(i) Secret part, key or mathematical construct from a pair of keys which together form the basis of Public Key Technologies. (See Public key)</p> <p>(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</p> <p>(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.</p> <p>(iv) (secret key - deprecated) (In a public key cryptosystem) that key of a user's key pair which is known only by that user.</p> <p>(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.</p>
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).

Term or Acronym	Explanatory notes
Protective Security	The total concept of administrative, personnel, physical, technical, computer and communication security.
PSM	Protective Security Manual
PSRR	Protective Security Risk Review
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>

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 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.

Term or Acronym	Explanatory notes
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
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

Term or Acronym	Explanatory notes
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.
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.

Term or Acronym	Explanatory notes
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:

www.iso.ch.8080/jtc1/sc27/27sd698a.htm

APPENDIX B - ORGANISATION PROOF OF IDENTITY FORM — USER DETAILS

Organisation Proof Of Identity — User Details Certificate Summary Information

Organisation Details

Organisation Name:

Department/Branch:

Contact Details

Name:

Title:

Business Address:

Business Telephone:

Business Email Address:

Total POI points:

ITEM	GIVEN		NOTE	
	Y	N		
Has a registration proforma completed?				
Have photocopies been taken of the organisation's POI documents?				
Has the organisation been advised how to access and read the Certificate Policy Statement?				
Has the organisation had the Certificate Policy Statement explained to them?				
Has a copy of this registration record been provided to the organisation?				

This record is to be attached to the front of a sealed envelope, containing the photocopies of the identification documents taken during the abovementioned user's registration interview.

(Interviewer's signature)

(Operator's signature)

Proof Of Identity form — Organisation

Organisation Proof of Identity — Identification POI Value 50 points each

DOCUMENTS	SEEN?		REF	PTS
	Y	N		
POI VALUE 50 POINTS EACH				
Certificate of registration of a company				
Strata Title certificate of registration				
Sale or purchase of business				
Liquidation notice				
A statement of transaction issued by a financial institution in the name of the company and less than 1 year old.				
Appointment of trustee				
Lease agreement of business property				
Rates notice of business property				
Certificate of change of company name				
	Total points:			

(Interviewer's signature)