

AusCERT Certification Practice Statement and Certificate Policy

AusCERT
The University of Queensland
QLD 4072
Australia

Version 1.0

TABLE OF CONTENTS

1. INTRODUCTION	10
1.1. Overview	10
1.2. Document Name and Identification	10
1.3. PKI Participants	11
1.3.1. Certification Authorities	11
1.3.2. Participant Organisations	11
1.3.3. Subscribers	11
1.3.4. Relying Parties	12
1.3.5. Other Participants	12
1.4. Certificate Usage	12
1.4.1. Appropriate Certificate Use	12
1.4.2. Prohibited Certificate Use	12
1.5. Policy Administration	13
1.5.1. Organisation Administering the Document	13
1.5.2. Contact Person	13
1.5.3. Person Determining CPS Suitability for the Policy	13
1.5.4. CPS Approval Procedures	13
1.6. Definitions and Acronyms	13
1.7. Legal	15
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	15
2.1. Repositories	15
2.2. Publication of Certificate Information	15
2.3. Time or Frequency of Publication	15
2.4. Access Controls on Repositories	16
3. IDENTIFICATION AND AUTHENTICATION	16
3.1. Naming	16
3.1.1. Types of Names	16
3.1.2. Need for Names to be Meaningful	17
3.1.3. Anonymity or Pseudo-anonymity of Subscribers	17
3.1.4. Rules for Interpreting Various name Forms	17
3.1.5. Uniqueness of Names	17
3.1.6. Recognition, Authentication, and Role of Trade marks	17
3.2. Initial Identity Validation	17
3.2.1. Method to Prove Possession of Private Key	18
3.2.2. Authentication of Organisation Identity	18

3.2.3.	Authentication of Individual Identity	19
3.2.4.	Non-Verified Subscriber Information	20
3.2.5.	Validation of Authority	20
3.2.6.	Criteria for Interoperation	20
3.3.	Identification and Authentication for Renewal Requests	20
3.3.1.	Identification and Authentication for Routines Renewal	20
3.3.2.	Identification and Authentication for Renewal After Revocation	20
3.4.	Identification and Authentication for Revocation Requests	20
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	20
4.1.	Certificate Application	20
4.1.1.	Who Can Submit a Certificate Application	21
4.1.2.	Enrollment Process and Responsibilities	21
4.2.	Certificate Application Processing	21
4.2.1.	Performing Identification and Authentication Functions	22
4.2.1.1.	Organisation Validated Certificate Validation	22
4.2.1.2.	Personal/Client Validated Certificate Validation	22
4.2.1.2.1.	Standard Personal/Client Validated Certificate	23
4.2.1.3.	Code Signing Certificate Validation	23
4.2.2.	Approval or Rejection of Certificate Applications	23
4.2.3.	Time to Process Certificate Applications	23
4.3.	Certificate Issuance	23
4.3.1.	CA Actions During Certificate Issuance	23
4.3.2.	Notification to Subscriber by the CA of Issuance of Certificate	24
4.3.3.	Notification of Certificate Issuance by the CA to Other Entities	24
4.4.	Certificate Acceptance	24
4.4.1.	Conduct Constituting Certificate Acceptance	24
4.4.2.	Publication of the Certificate by the CA	24
4.5.	Key Pair and Certificate Usage	24
4.5.1.	Subscriber Private Key and Certificate Usage	24
4.5.2.	Relying Party Public Key and Certificate Usage	24
4.6.	Certificate Renewal	25
4.6.1.	Circumstances for Certificate Renewal	25
4.6.2.	Who May Request Renewal	25
4.6.3.	Processing Certificate Renewal Requests	25
4.6.4.	Notification of New Certificate Issuance to Subscriber	25
4.6.5.	Conduct Constituting Acceptance of a Renewal Certificate	25
4.6.6.	Publication of the Renewal Certificate by the CA	25
4.6.7.	Notification of Certificate Issuance by the CA to other Entities	25
4.7.	Certificate Re-key	25

4.8.	Certificate Modification.....	25
4.8.1.	Circumstance for Certificate Modification.....	25
4.8.2.	Who May Request Certificate Modification	25
4.8.3.	Processing Certificate Modification Requests	25
4.8.4.	Notification of New Certificate Issuance to Subscriber	25
4.8.5.	Conduct Constituting Acceptance of Modified Certificate	25
4.8.6.	Publication of the Modified Certificate by the CA.....	26
4.8.7.	Notification of Certificate Issuance by the CA to Other Entities	26
4.9.	Certificate Revocation and Suspension	26
4.9.1.	Circumstances for Revocation.....	26
4.9.2.	Who can Request Revocation	27
4.9.3.	Procedure for Revocation Request.....	27
4.9.4.	Revocation Request Grace Period	27
4.9.5.	Revocation Checking Requirement for Relying Parties	27
4.9.6.	Time Within Which CA Must Process the Revocation Request	27
4.9.7.	CRL Issuance Frequency	27
4.9.8.	Maximum Latency for CRLs	27
4.9.9.	On-line Revocation/Status Checking Availability	27
4.9.10.	On-line Revocation Checking Requirements.....	28
4.9.11.	Other Forms for Revocation Advertisements available.....	28
4.9.12.	Special Requirements Re-key Compromise	28
4.9.13.	Circumstances for Suspension	28
4.9.14.	Who can Request Suspension	28
4.9.15.	Procedure for Suspension Request	28
4.9.16.	Limits on Suspension Period	28
4.10.	Certificate Status Services	28
4.10.1.	Operational Characteristics	28
4.10.2.	Service Availability	28
4.10.3.	Optional Features	28
4.11.	End of Subscription.....	28
4.12.	Key Escrow and Recovery	28
5.	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	29
5.1.	Physical Security Controls	29
5.1.1.	Site Location and Construction.....	29
5.1.2.	Physical Access	29
5.1.3.	Power and Air Conditioning.....	29
5.1.4.	Water Exposures	29
5.1.5.	Fire Prevention and Protection	29
5.1.6.	Media Storage	29

5.1.7.	Waste Disposal	30
5.1.8.	Off-site Backup	30
5.2.	Procedural Controls	30
5.2.1.	Trusted Personnel	30
5.2.2.	Personnel Controls.....	30
5.2.3.	Identification and Authentication for Trusted Personnel	30
5.2.4.	Personnel Responsibilities	30
5.3.	Personnel Security Controls.....	30
5.3.1.	Qualifications, Experience, and Clearance Requirements	30
5.3.2.	Training Requirements	31
5.3.3.	Retraining Frequency and Requirements.....	31
5.3.4.	Job Rotation Frequency and Sequence.....	31
5.3.5.	Sanctions for Unauthorised Actions.....	31
5.3.6.	Independent Contractor Requirements	31
5.3.7.	Documentation Supplied to Personnel.....	31
5.4.	Audit Logging Procedures.....	31
5.4.1.	Types of Events Recoded	31
5.4.2.	Frequency of Processing Log	32
5.4.3.	Retention Period of Audit Log.....	32
5.4.4.	Protection of Audit Log	32
5.4.5.	Audit Log Backup Procedures	32
5.4.6.	Audit Collection System	32
5.4.7.	Notification to Event-Causing Subject.....	32
5.4.8.	Vulnerability Assessments.....	32
5.5.	Records archival.....	32
5.5.1.	Types of records archived	32
5.5.2.	Retention period for archive	33
5.5.3.	Protection of archive	33
5.5.4.	Archive backup procedures	33
5.5.5.	Requirements for time-stamping of records	33
5.5.6.	Archive collection system	33
5.5.7.	Procedures to obtain and verify archive information.....	33
5.6.	Key changeover.....	33
5.7.	Compromise and disaster recovery.....	33
5.7.1.	Incident and compromise handling procedures.....	33
5.7.2.	Computing resources, software, and/or data are corrupted.....	33
5.7.3.	Business continuity capabilities after a disaster	34
5.8.	CA termination.....	34
6.	TECHNICAL SECURITY CONTROLS.....	34

6.1.	Key pair generation and installation	34
6.1.1.	Key pair generation	34
6.1.2.	Certificate and Certificate Chain delivery to Subscriber	35
6.1.2.1.	Server Certificate	35
6.1.2.2.	Delivery of other Certificates	35
6.1.3.	Public key delivery to Certificate issuer	35
6.1.4.	CA public key delivery to Relying Parties	35
6.1.5.	Key sizes	35
6.1.6.	Public key parameters generation and quality checking	36
6.1.7.	Key usage purposes (as per X.509 v3 key usage field)	36
6.2.	Private Key Protection and Cryptographic Module Engineering Controls	36
6.2.1.	Cryptographic module standards and controls	36
6.2.2.	Private key (n out of m) multi-person control	36
6.2.3.	Private key escrow	36
6.2.4.	Private key backup	36
6.2.5.	Private key archival	36
6.2.6.	Private key transfer into or from a cryptographic module	37
6.2.7.	Private key storage on cryptographic module	37
6.2.8.	Method of activating private key	37
6.2.9.	Method of deactivating private key	37
6.2.10.	Method of destroying private key	37
6.2.11.	Cryptographic Module Rating	37
6.3.	Other aspects of key pair management	37
6.3.1.	Public key archival	37
6.3.2.	Certificate operational periods and key pair usage periods	37
6.4.	Activation data	37
6.4.1.	Activation data generation and installation	37
6.4.2.	Activation data protection	37
6.4.3.	Other aspects of activation data	38
6.5.	Computer security controls	38
6.5.1.	Specific computer security technical requirements	38
6.5.2.	Computer security rating	38
6.6.	Life cycle technical controls	38
6.6.1.	System development controls	38
6.6.2.	Security management controls	38
6.6.3.	Life cycle security controls	38
6.7.	Network security controls	38
6.8.	Time-stamping	38
7.	CERTIFICATE, CRL, AND OCSP PROFILES	38

7.1.	Certificate profile.....	39
7.1.1.	Version number(s)	39
7.1.2.	Certificate extensions.....	39
7.1.2.1.	Key Usage Extension field.....	39
7.1.2.2.	Extension Criticality Field	39
7.1.2.3.	Basic Constraints Extension	39
7.1.3.	Algorithm object identifiers	40
7.1.4.	Name forms	40
7.1.5.	Name constraints	40
7.1.6.	Certificate policy object identifier	40
7.1.7.	Usage of Policy Constraints extension.....	40
7.1.8.	Policy qualifiers syntax and semantics.....	40
7.1.9.	Processing semantics for the critical Certificate Policies extension	40
7.2.	CRL profile	40
7.2.1.	Version number(s)	40
7.2.2.	CRL and CRL entry extensions	41
7.3.	OCSP profile	41
7.3.1.	Version Number(s).....	41
7.3.2.	OCSP Extensions	41
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	41
8.1.	Frequency or Circumstances of Assessment.....	41
8.2.	Identity/Qualifications of Assessor.....	41
8.3.	Assessor's Relationship to Assessed Entity	41
8.4.	Topics Covered by Assessment.....	42
8.5.	Actions Taken as a Result of Deficiency.....	42
8.6.	Communication of Results	42
9.	OTHER BUSINESS AND LEGAL MATTERS	42
9.1.	Fees.....	42
9.1.1.	Certificate Issuance or Renewal Fees	42
9.1.2.	Certificate Access Fees.....	42
9.1.3.	Revocation or Status Information Access Fees.....	42
9.1.4.	Fees for Other Services	42
9.1.5.	Refund Policy.....	43
9.2.	Financial Responsibility	43
9.2.1.	Insurance Coverage.....	43
9.2.2.	Other Assets.....	43
9.2.3.	Insurance or Warranty Coverage for End-Entities	43
9.3.	Confidentiality of Business Information.....	43
9.3.1.	Scope of Confidential Information.....	43

9.3.2.	Information Not Within the Scope of Confidential Information.....	43
9.3.3.	Responsibility to Protect Confidential Information	43
9.3.4.	Disclosure Pursuant to Judicial or Administrative Process	43
9.4.	Privacy of Personal Information	44
9.4.1.	Privacy Plan.....	44
9.4.2.	Information Treated as Private	44
9.4.3.	Information Not Deemed Private	44
9.4.4.	Responsibility to Protect Private Information.....	44
9.4.5.	Disclosure Pursuant to Judicial or Administrative Process	44
9.4.6.	Other Information Disclosure Circumstances	44
9.5.	Intellectual Property Rights	44
9.5.1.	Certificates.....	44
9.5.2.	Copyright	45
9.5.3.	Trade marks.....	45
9.6.	Representations and Warranties.....	45
9.6.1.	CA Representations and Warranties	46
9.6.2.	Participant Organisation Representations and Warranties	47
9.6.3.	RA Representations and Warranties	47
9.6.4.	Subscriber Representations and Warranties.....	47
9.6.5.	Relying Party Representations and Warranties.....	49
9.6.6.	Representations and Warranties of Other Participants.....	49
9.7.	Limitations of Liability.....	49
9.8.	Indemnities	50
9.8.1.	Participant Organisation Indemnity to AusCERT	50
9.8.2.	Subscriber Indemnity to AusCERT	50
9.8.3.	Subscriber Indemnity to Relying Parties	51
9.9.	Term and Termination.....	51
9.9.1.	Term	51
9.9.2.	Termination.....	51
9.9.3.	Effect of Termination and Survival	51
9.10.	Individual notices and Communications with Participants	51
9.11.	Amendments	51
9.11.1.	Procedure for Amendment	52
9.11.2.	Notification Mechanism and Period	52
9.11.3.	Circumstances Under Which OID Must be Changed.....	52
9.12.	Dispute Resolution Procedures.....	52
9.13.	Governing Law	52
9.14.	Jurisdiction	52
9.15.	Miscellaneous Provisions.....	52

9.15.1.	Interpretation.....	52
9.15.2.	Assignment.....	53
9.15.3.	Severability	53
9.15.4.	Enforcement and waiver.....	53
9.15.5.	Force Majeure.....	53
9.16.	Other Provisions	53
9.16.1.	Refusal to Issue a Certificate.....	53
9.16.2.	Legality of Information	53
9.16.3.	Subscriber Liability to Relying Parties.....	53
9.16.4.	Duty to Monitor Agents.....	54
9.16.5.	Conditions of usage of the AusCERT Repository and Web site.....	54
9.16.6.	Accuracy of Information.....	54
9.16.7.	Non-Verified Subscriber Information.....	54
APPENDIX A	55
APPENDIX B	56
APPENDIX C	57
APPENDIX D	59

1. INTRODUCTION

AusCERT is a division of The University of Queensland ABN 63 942 912 684.

AusCERT Certification Authority Certificate Services ("AusCERT") is a Certification Authority ("CA") that issues Certificates to various subscribing entities which are part of the educational or research communities. AusCERT performs functions associated with public key operations which include receiving application requests for, issuing, revoking and renewing Certificates and the maintenance, issuance, and publication of Certificate Revocation Lists ("CRLs") and an Online Certificate Status Protocol ("OCSP").

The AusCERT CA infrastructure is hosted and operated by Comodo CA Ltd ("Comodo").

1.1. Overview

This document is the AusCERT Certification Practice Statement ("CPS"). The AusCERT CPS outlines the legal, commercial and technical principles and practices that AusCERT employs in approving, issuing, using, and managing certification services. This includes approving, issuing, using and managing Certificates and maintaining a X.509 Certificate based public key infrastructure ("PKIX"). AusCERT may update and supplement this CPS with amendments in order to provide for additional product offerings and to comply with certain regulatory or industry standards and requirements.

This CPS describes AusCERT's Certificate issuance processes, business operations, and repository operations. The CPS is only one of many documents that are relevant to AusCERT's Certificate issuance practices. Other important documents include the AusCERT Subscriber Agreement, the Relying Party Agreement, and other ancillary agreements that are posted on the AusCERT Repository. These documents obligate parties using or relying on an AusCERT Certificate to meet a certain minimum criteria prior to their use or reliance on an AusCERT Certificate.

AusCERT's CPS is also a means to notify the public and relevant parties of the roles and responsibilities involved in Certificate based practices within the AusCERT PKI Certificate Service. The CPS is formatted and maintained in accordance with IETF PKIX RFC 3647 and is divided into separate sections that cover the practices and procures for applying for, identifying, issuing, and revoking Certificates along with information about AusCERT's security controls and auditing process.

AusCERT extends, under agreement, membership of AusCERT Certificate Service to approved third parties known as Participant Organisations. The international network of Participant Organisations share AusCERT's policies, practices, and CA infrastructure to issue AusCERT Certificates. Certificates will be managed and issued using the Certificate Services Manager (CSM) web provisioning interface or any other mechanism made available by AusCERT. Each Participant Organisation will appoint individual officers of their Organisations to act as Registration Authorities ("RAs"). RAs carry out various functions of the Participant Organisations, as set out in this CPS.

1.2. Document Name and Identification

This document is the AusCERT CPS version 1.0, which was approved for publication on 18 October 2011 by the AusCERT Certificate Policy Authority. The CPS is a public statement of the practices of AusCERT and the conditions of issuance, revocation and renewal of a Certificate issued under AusCERT's PKI Certificate Service hierarchy. Revisions to this document have been made as follows:

Date	Changes	Version

Revisions not denoted "significant" are those deemed by the AusCERT Certificate Policy Authority to have minimal or no impact on Subscribers and Relying Parties using Certificates, the CRLs and the OCSP issued by AusCERT. Insignificant revisions may be made without changing the version number of this CPS.

The AusCERT Certificate Policy Authority may be contacted via email at cspa@auscert.org.au.

This CPS is identified by the following unique registered object identifier (OID):

1.3.6.1.4.1.23485.5.1.1.0

ISO assigned	1
Organisation acknowledged by ISO	3
US Department of Defense	6
Internet	1
Internet Private	4
IANA registered private enterprises	1
AusCERT	23485
Certificate Service	5
CPS	1
Major Version	1
Minor version	0

1.3. PKI Participants

1.3.1. Certification Authorities

The term “Certification Authority (CA)” is a generic term used to describe entities that are allowed to issue public key Certificates. The AusCERT CA:

- Conforms its operations to this CPS and may from time to time be modified by amendments published in the AusCERT Repository cs.auscert.org.au/repository/
- Issues and publishes Certificates in a timely manner in accordance with the issuance times set forth in this CPS,
- Revokes Certificates upon receipt of a valid revocation request from a person authorised to request revocation,
- Maintains and updates its OCSP on a regular basis and in a timely manner, in accordance with the applicable Certificate Policy and as described in this CPS,
- Publishes CRLs on a regular basis, in accordance with the applicable Certificate Policy and as described in this CPS,
- Distributes issued Certificates in accordance with the methods detailed in this CPS,
- Updates CRLs in a timely manner as detailed in this CPS, and
- Notifies Subscribers and/or Participant Organisation via email of expiring AusCERT issued Certificates (for a period disclosed in this CPS).

1.3.2. Participant Organisations

AusCERT appoints certain partners to assist in or perform the management and issuance of Certificates, including the verification and identification processes. Appointment as a Participant Organisation is subject to AusCERT's sole discretion.

Participant Organisations, through their approved RAs, may accept or reject Certificate applications, validate information that will be contained in a Certificate, and request the issuance of a Certificate. Participant Organisations are contractually obligated to follow AusCERT's CPS when validating and issuing Certificates to Subscribers.

1.3.3. Subscribers

Subscribers are individuals, companies, or other entities that use AusCERT's PKI services to provide supported transactions and communications. Subscribers are identified in and have the private key corresponding to the public key listed in an issued Certificate. Prior to being issued a Certificate, an Applicant (a potential Subscriber) must submit an application accompanied by certain verification information. AusCERT will only issue a Certificate to an Applicant after the Applicant has been approved and verified by AusCERT or a Participant Organisation, through its RA.

In certain circumstances, AusCERT may issue a Certificate to an individual or entity that is different from the entity which actually applied for the Certificate. In such circumstances, the Subject of the Certificate will be the entity whose credentials have been submitted, and the term Subscriber shall apply to the entity which contracted with AusCERT for the issuance of the Certificate. Regardless of the Subject listed in the Certificate, the Subscriber always has the responsibility of ensuring that the Certificate is only used appropriately.

1.3.4. Relying Parties

Relying Parties use AusCERT's PKI Certificate Services to perform certain transactions, communications, or functions and may reasonably rely on issued Certificates that contain a verifiable reference to a public key that is listed in the Subscriber Certificate. AusCERT's SSL Certificate products are not intended to be used in Monetary Transactions, and a party who relies on such a Certificate does not qualify as a Relying Party.

Certificates do not guarantee that a Certificate holder has good intentions or that the Certificate holder will be an ethical business operation. Relying Parties should always independently examine each Certificate holder to determine whether the Certificate owner is ethical and trustworthy.

1.3.5. Other Participants

Not applicable

1.4. Certificate Usage

A Certificate is formatted data that cryptographically binds an identified Subscriber to a public key. A Certificate allows an entity taking part in an electronic transaction to prove its identity to the other participants in such transaction. Certificates may be issued for individuals, Organisations, government entities, educational institutions, or infrastructure components such as firewalls, routers, or other security devices.

1.4.1. Appropriate Certificate Use

Depending on the Certificate type, the Certificates issued from AusCERT may only be used for authentication, encryption, access control, code signing and digital signature purposes.

AusCERT uses third party domain name registrars and directories to assist with application validation in order to provide increased speed of issuance. Where possible, AusCERT's Participant Organisation's or a third party's directories will be used to confirm the right to use the domain name used in the application. If the directory cannot be used to sufficiently validate a Certificate Applicant, further validation processes may be used which may include an out of bands validation of the Applicant's submitted information.

See Appendix B for further information on types of Certificates issued by AusCERT.

1.4.2. Prohibited Certificate Use

Certificates may only be used in accordance with their intended purpose and in compliance with all applicable laws and regulations. Certificates may not be used to complete or assist in performing any transaction that is prohibited by law.

Each party using or relying on a Certificate shall be bound by and comply with the terms and conditions set forth in the applicable agreement between the party and AusCERT. Certificates do not guarantee that a Certificate holder has good intentions or that the Certificate holder will be an ethical business operation.

Certificates may not be used for any application requiring fail-safe performance systems such as the operation of nuclear power facilities, air traffic control systems, weapon control systems, or any other system where a failure of the system could cause any form of damage.

SSL Certificates issued by AusCERT may not be used to conduct Monetary Transactions.

1.5. Policy Administration

1.5.1. Organisation Administering the Document

This CPS and any related documents, agreements, or policy statements referenced herein are maintained and administered by the AusCERT Certificate Policy Authority.

1.5.2. Contact Person

AusCERT Certificate Policy Authority
AusCERT
The University of Queensland
QLD 4072
Telephone: +61 7 3365 4417
Australia

Email: cspa@auscert.org.au

1.5.3. Person Determining CPS Suitability for the Policy

The suitability and applicability of AusCERT's CPS is reviewed and approved by the AusCERT Certificate Policy Authority.

1.5.4. CPS Approval Procedures

AusCERT's CPS and any significant amendments made to it are reviewed and approved by the AusCERT Certificate Policy Authority and legal department. Amendments to the CPS may be made by reviewing and updating the entire CPS or by publishing an addendum. The current version of the CPS is always made available to the public through the AusCERT Repository which can be accessed online at cs.auscert.org.au/repository/. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in Section 5.4 of this CPS.

1.6. Definitions and Acronyms

Acronyms:

CA	Certification Authority
CCM	Comodo Certificate Manager
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSM	Certificate Services Manager
CSR	Certificate Signing Request
EPKI	Enterprise Public Key Infrastructure Manager
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MDC	Multiple Domain Certificate
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Certificates)
PKCS	Public Key Cryptography Standard

RA	Registration Authority
SGC	Server Gated Cryptography
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

Definitions:

Applicant	The Applicant is an entity applying for a Certificate.
AusCERT Repository	The AusCERT Repository is located at cs.auscert.org.au/repository/
Certificate	A digital file that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, and contains a serial number.
Certificate Policy	The Certificate policy is a statement of the issuer that corresponds to the prescribed usage of a Certificate within an issuance context.
Certificate Services Manager	The Certificate Services Manager is a web provisioning interface based on CCM and developed by Comodo to accommodate the AusCERT customers' requirement for hierarchical self provisioning and management of certificates.
Monetary Transactions	Any online financial transaction which is secured or encrypted by a Certificate issued from AusCERT Sub CA rooted to Comodo. Financial transactions include cash bank transfer and credit/debit Card transactions.
Subscriber	The Subscriber is an entity that has been issued a Certificate.
Subscriber Agreement	The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the Certificate product type as presented during the product online order process.
Subject	The Subject of a Certificate is an entity that the Certificate relates to.
Participant Organisation	An Organisation that partners with AusCERT to request and use Certificates issued under this CPS.
Participant Agreement	The Participant Organisation Agreement is a service agreement that must be signed by a Participant Organisation before Certificates within the AusCERT PKI Certificate Service can be requested and issued to their Organisation.
Registration Authority	Personnel appointed by Participant Organisation to request and issue certificates on behalf of the Participant Organisation.
Relying Party	The Relying Party is an entity that relies upon the information contained within the Certificate.
Relying Party Agreement	The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at cs.auscert.org.au/repository/

1.7. Legal

For legal liability of AusCERT and other parties under the provisions of this CPS, please refer to section 9.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This CPS is only one of a set of documents relevant to the AusCERT's certification services. The list of documents below is a list of other documents that this CPS will from time to time mention. The list is not exhaustive. The document name, location of, and status, whether public or private, are detailed below. The AusCERT Repository can be found at cs.auscert.org.au/repository/.

Document	Status	Location
AusCERT Certification Practice Statement	Public	AusCERT Repository
Subscriber Agreement	Public	AusCERT Repository
Relying Party Agreement	Public	AusCERT Repository
Participant Organisation Agreement	Confidential	Presented to partners accordingly

2.1. Repositories

AusCERT publishes this CPS, its Subscriber Agreements, and the Relying Party Agreement in the official AusCERT Repository. The AusCERT Certificate Policy Authority maintains the AusCERT Repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in this CPS.

AusCERT makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated, and correct information. However, AusCERT cannot accept any liability beyond the limits set forth in this CPS.

Parties accessing the AusCERT Repository agree with the provisions of this CPS and any other conditions of usage that AusCERT may make available. Parties demonstrate acceptance of this CPS and the other terms and conditions that may apply by using an AusCERT issued Certificate.

Failure to comply with the conditions herein or posted on the AusCERT website may result in the termination of the relationship between AusCERT and the party.

2.2. Publication of Certificate Information

Certificate information is published by AusCERT's issuance of the Certificate and in accordance with the provisions of this CPS that are relevant to such a Certificate. Revoked Certificate information is published through AusCERT's OCSP operations.

An updated CRL is published by Comodo every 24 hours. Under special circumstances the CRL may be published more frequently. Users and Relying Parties are strongly urged to consult the directories of revoked Certificates at all times prior to relying on information featured in a Certificate.

2.3. Time or Frequency of Publication

Updates to the CPS are published in accordance with Section 9.12. Updates to the Subscriber Agreement, Relying Party Agreements, and other agreements posted on the AusCERT Repository are published as often as necessary. Certificates are published upon issuance.

Certificate information is published in accordance with the provisions of the CPS relevant to such a Certificate. CRLs are issued by Comodo every 24 hours and include a monotonically increasing sequence number for each CRL issued. Under special circumstances, AusCERT may publish new CRLs prior to the expiration of the current CRL. Each CRL is valid only for the 24 hours following its publication or until an updated CRL has been published, whichever comes first.

Typically, AusCERT updates its OCSP every 24 hours. Under special circumstances the OCSP may be more frequently. All parties are strongly urged to always consult the OCSP prior to relying on information featured in a Certificate.

2.4. Access Controls on Repositories

The information published in the AusCERT Repository is public information and may be accessed freely by anyone visiting the site, provided they agree to the site's terms and conditions as posted thereon. Read-only access to the information is unrestricted. AusCERT has implemented logical and physical security measures aimed at preventing unauthorised additions, modification, or deletions of repository entries.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of Names

AusCERT Certificates are issued with an X.501 compliant non-null Distinguished Name (DN) in the Issuer and Subject Fields. Issuer Distinguished Names may consist of a combination of the following Components (refer to Appendix D for CN details for each type of certificate):

Attribute	Abbr.	Value
Common Name	CN	AusCERT Certificate Services
Organisation	O	AusCERT
Country	C	AU

Certificate Distinguished Names may consist of a combination of the following Components:

Attribute	Abbr.	Value
Common Name	CN	The Common Name which could be the name of the Subscriber or domain name for which the Certificate has been issued (required)
Organisation	O	The Organisation (required)
Organisational Unit	OU	Certificates may be multiple OU attributes. The attributes may include: Organisation information Copyright information References to the terms and conditions of use Description of the Certificate Certificate warranty information Verification or validation information Issuance and/or hosting information Special Certificate notes (optional)
Country	C	The two letter ISO country code of the Organisation (required)
Locality	L	Locality of the Organisation (optional)
State or Province	S	State of the Organisation (optional)
Street	STREET	Street address (optional)
Postal code	PostalCode	Postal code (optional)
Email address	E	Email address for Email Certificates

Enhanced naming is the usage of an extended Organisation field in an X.509v3 Certificate. Information contained in the Organisational unit field is also included in the Certificate Policy extension that AusCERT may use.

AusCERT Certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the Certificate and any disclaimers of warranty that may apply. The lack of such information does not mean it does not apply to that Certificate.

To communicate information AusCERT may use:

- An Organisational unit attributes.
- An AusCERT standard resource qualifier to a Certificate policy.
- Proprietary or other extensions.

3.1.2. Need for Names to be Meaningful

AusCERT uses non-ambiguous designations and commonly used semantics to identify both the issuer of the Certificate and the Subject of the Certificate.

3.1.3. Anonymity or Pseudo-anonymity of Subscribers

AusCERT does not intentionally issue anonymous or pseudo-anonymous names. However, email Certificate Subscribers are validated by the Participant Organisation prior to the Certificate's issuance, this process is based on the Participant Organisation naming conventions for their users and, as a result, may contain an anonymous or pseudo-anonymous name.

3.1.4. Rules for Interpreting Various name Forms

Distinguished Names in Certificates are X.501 compliant. For information on how X.501 Distinguished Names are interpreted, please see RFC 2253 and RFC 2616.

3.1.5. Uniqueness of Names

The Serial Number of an AusCERT-issued Certificate is unique for each Subscriber, uniqueness is ensured through an automated process.

3.1.6. Recognition, Authentication, and Role of Trade marks

Through its Subscriber Agreements, AusCERT prohibits the use of a name or symbol that infringes upon the intellectual property rights of another. However, AusCERT does not verify or check the name appearing in a Certificate for non-infringement. Subscribers are solely responsible for ensuring the legality of any information presented for use in an AusCERT-issued Certificate. AusCERT Subscribers represent and warrant that when submitting an application to AusCERT and when using a domain and distinguished name (and all other Certificate application information) that they are not interfering with or infringing any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortuous interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

AusCERT does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property or a domain's use of any infringing material. AusCERT, in its sole discretion and without any liability, may reject an application or revoke a Certificate, based on any intellectual property infringement claims or ownership disputes.

3.2. Initial Identity Validation

Upon receipt of an application for a Certificate and based on the submitted information, AusCERT or the Participant Organisation RA confirms the following information:

- The Certificate Applicant is the same person as the person identified in the Certificate request.

- The Certificate Applicant holds the private key corresponding to the public key to be included in the Certificate.
- The information to be published in the Certificate is accurate, except for non-verified Subscriber information.
- Any agents who apply for a Certificate listing the Certificate Applicant's public key are duly authorised to do so.

Verification of a digital signature is used to determine that:

- the private key corresponding to the public key listed in the signer's Certificate created the digital signature, and
- the signed data associated with this digital signature has not been altered since the digital signature was created.

In all types of AusCERT Certificates, the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify AusCERT of any changes that would affect the validity of the Certificate. Failure to comply with the obligations as set out in the Subscriber Agreement will result in the revocation of the Subscriber's Certificate without further notice to the Subscriber. Subscriber shall still be required to pay any applicable charges and fees as specified in the relevant Subscriber Agreement.

3.2.1. Method to Prove Possession of Private Key

Every Applicant must demonstrate that it holds the private key corresponding to the public key that will be included in the Certificate. To prove possession, the Applicant must submit a digitally signed PKCS#10 to AusCERT or Participant Organisation or provide another cryptographically equivalent demonstration.

3.2.2. Authentication of Organisation Identity

The following elements are critical information elements for an AusCERT Certificate issued to an Organisation. Those elements marked with PUBLIC are present within an issued Certificate and are therefore within the public domain. Those elements not marked with PUBLIC that constitute confidential information remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organisation (PUBLIC)
- Organisational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- ABN, VAT-number or equivalent (if applicable) (PUBLIC)
- Company / DUNS number (if available)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone (PUBLIC)
- Billing contact full name, email address and telephone (PUBLIC)
- Organisational contact full name, email address and telephone (PUBLIC)
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public key (PUBLIC)
- Proof of existence and Organisational status of the Organisation
- Subscriber Agreement, signed (if applying out of bands)

Documentation requirements for Organisational Applicants include any / all of the following:

- Articles of Association
- Business License
- Certificate of Compliance

- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Tax Certification
- Corporate Charter
- Official letter from an authorised representative of a government Organisation
- Official letter from office of Dean or Principal (for Educational Institutions)

AusCERT may accept at its discretion other official Organisational documentation supporting an application.

Each Certificate is validated according to the level of security required for the issued Certificate as explained more fully in Section 4.2

AusCERT may use the services of a third party to confirm information on a business entity that applies for a Certificate. AusCERT accepts confirmation from third party Organisations, other third party databases and government entities.

AusCERT's controls may also include ASIC transcripts (or equivalent in jurisdictions other than Australia) that confirm the registration of the Applicant company and state the members of the board, the management and Directors representing the company.

Applicants shall solely be responsible for the legality of the information they present for use in Certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

Each administrator contact, billing contact and Organisational contact must operate in compliance with this CPS. However, by stipulating an administrator contact, a billing contact and an Organisational contact, a Participant Organisation accepts full responsibility for those contacts' actions.

3.2.3. Authentication of Individual Identity

The following elements are critical information elements for an AusCERT Certificate issued to an individual:

- Legal Name of the Individual (PUBLIC)
- Organisational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- ABN, VAT-number or equivalent (if applicable) (PUBLIC)
- Server Software Identification
- Payment Information (if applicable)
- Contact information including full name, email address and telephone
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public key (PUBLIC)
- Subscriber Agreement, signed (if applying out of bands)

Documentation requirements for Individual Applicants shall include identification elements such as:

- Passport
- Driving License
- Bank statement
- Documents accepted under the Financial Transaction Reports Act 1988 (FTR Act), Identification Record for a Signatory to an Account, '100 Point Check' Special Provisions (202) (www.austrac.gov.au/files/201_point_check.pdf).
- Participant Organisation vouching for the Applicant's identity as described in its Organisational records database.

AusCERT may accept, in its sole discretion, other official documentation supporting an application.

Each Certificate is validated according to the level of security required for the issued Certificate as explained more fully in Section 4.2

3.2.4. Non-Verified Subscriber Information

AusCERT does not validate any information not listed as being validated under Section 4.2.

3.2.5. Validation of Authority

Participant Organisations will appoint and validate individuals with authority to request and approve Certificates on behalf of their Organisation, these authorised personnel as described in 1.3.2 will have the authority to act on behalf of their users and domain owner.

Validation information about Participant Organisation's authorised personnel and domain ownership will be made available to AusCERT in writing.

Appointed personnel must provide copies and originals of proof of identity in person to a Justice of Peace or to previously appointed and validated authorised personnel and have the copies certified as true copies. Appointed personnel must also complete an "Application to be an RA" form and sign it in the presence of a Justice of Peace or previously appointed and validated authorised personnel. Once the RA application has been accepted these personnel can act on behalf of their Organisation as 'validated authorised personnel' for subsequent RA applications. The "Application to be an RA" form is available at the AusCERT Repository (cs.auscert.org.au/repository/).

By appointing an RA, the appointing Participant Organisation accepts full responsibility for the RA's actions.

The Subscriber shall control and be responsible for the data supplied to the Participant Organisation's agent and to AusCERT. The Subscriber must promptly notify AusCERT and Participant Organisation of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

3.2.6. Criteria for Interoperation

AusCERT does not appoint third party CAs and does not allow other CAs to sign to its root Certificates.

3.3. Identification and Authentication for Renewal Requests

3.3.1. Identification and Authentication for Routines Renewal

Renewal application requirements and procedures are the same as those requirements and procedures implemented for the application validation and issuance of new customers.

3.3.2. Identification and Authentication for Renewal After Revocation

Renewal after revocation is only permitted if the Certificate was not revoked because of (i) a mistake in the party to whom the Certificate was issued, (ii) a breach of the Subscriber Agreement, (iii) a material misrepresentation by the Subscriber, or (iv) any other reason that could potentially cause harm to AusCERT's trusted status.

3.4. Identification and Authentication for Revocation Requests

Prior to revoking a Certificate, AusCERT or the Participant Organisation RA verifies that the revocation was requested by the Certificate Subscriber or the Participant Organisation authorised personnel. The revocation request can be sent by the administrator contact associated with the Certificate application. AusCERT or the Participant Organisation RA may, if necessary, also request that the revocation request be made by either the Organisational contact or billing contact. Upon receipt of the revocation request, AusCERT or the Participant Organisation RA will request confirmation of out of bands contact details, for example by telephone, signed email or by fax from the known administrator.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

AusCERT Certificates are issued to Organisations and individuals who submit a Certificate application and successfully complete the required validation procedures described herein. Prior to the issuance of a Certificate, AusCERT or the Participant Organisation RA will validate an application in accordance with

this CPS. Validation of the application may involve the request by AusCERT or the Participant Organisation RA for the Applicant to provide relevant official documentation supporting the application.

4.1.1. Who Can Submit a Certificate Application

Certificate applications may be submitted by an individual or an authorised representative of a Participant Organisation or other entity who is the subject of the Certificate. An authorised agent of an Applicant may submit a Certificate on the Applicant's behalf.

4.1.2. Enrollment Process and Responsibilities

Applicants may apply online, through email, or through written request for a Certificate. All Certificate applications are validated prior to issuing the Certificate. The enrollment process may include:

- Generating a RSA key pair and demonstrating to AusCERT ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR), this process can be done automatically by the Participant Organisation on behalf of its users in the case of bulk issuing of end entity Certificates.
- Making all reasonable efforts to protect the integrity the private key half of the key pair
- Submitting to AusCERT or Participant Organisation a Certificate application, including application information as detailed in this CPS, a public key half of a key pair, and agreeing to the terms of the relevant Subscriber Agreement
- Providing proof of identity through the submission of official documentation as requested by AusCERT or a Participant Organisation RA during the enrolment process

Additional documentation in support of the application may be required by AusCERT or the Participant Organisation RA in its sole discretion in order to assist AusCERT or the Participant Organisation RA in verifying the identity of the Applicant. Upon verification of identity, AusCERT issues the Certificate and sends a notice to the Applicant. The Applicant downloads and installs the Certificate to its device. The Applicant must notify AusCERT and/or Participant Organisation of any inaccuracy or defect in a Certificate promptly after receipt of the Certificate or earlier notice of informational content to be included in the Certificate.

The following steps describe the milestones to issue a Secure Server Certificate:

- a) The Applicant fills out the online request on AusCERT's web site and the Applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, Organisational information, country code, verification method and billing information, if applicable. AusCERT or Participant Organisation RAs may accept CSRs via email at their discretion or may generate the CSRs on behalf of their Organisation.
- b) The Applicant accepts the on line or out of band Subscriber Agreement.
- c) The Applicant submits the required information to AusCERT or Participant Organisation.
- d) The Applicant pays the Certificate fees, or the fees have been paid by their Organisation as part of the Participant Organisation Agreement.
- e) AusCERT or the Participant Organisation RA verifies the submitted information using third party databases, Government records or other methods at AusCERT's sole discretion.
- f) Upon successful validation of the application information, AusCERT or Participant Organisation may issue the Certificate to the Applicant using the Certificate Services Manager web provisioning interface or any other mechanism made available by AusCERT. Should the application be rejected, AusCERT or Participant Organisation will alert the Applicant that the application has been unsuccessful.
- g) Renewal is conducted as per the procedures outlined in this CPS and the official AusCERT websites.
- h) Revocation is conducted as per the procedures outlined in this CPS.

4.2. Certificate Application Processing

Prior to the issuance of a Certificate AusCERT will validate an application in accordance with this CPS which may involve the request by AusCERT or Participant Organisation RA to the Applicant for relevant official documentation supporting the application.

From time to time, AusCERT may modify the requirements related to application information for individuals, to respond to AusCERT's requirements, the business context of the usage of a Certificate, or as prescribed by law.

4.2.1. Performing Identification and Authentication Functions

Applications for AusCERT Certificates are supported by appropriate documentation to establish the identity of an Applicant as described in Section 3.2. AusCERT or Participant Organisation RA may use any means of communication at its disposal to ascertain the identity of an Organisational or individual Applicant. AusCERT reserves the right of refusal in its absolute discretion.

Prior to issuing a Certificate, AusCERT employs controls to validate the identity of the Subscriber information featured in the Certificate application. Such controls are indicative of the product type described in Appendix B. Controls listed below are used for Organisational validated Certificate types (including SSL, SGC SSL, Wildcard, MD, UC and Code Signing Certificates) and Personal Validated Certificates:

4.2.1.1. Organisation Validated Certificate Validation

Validation of Organisation validated Certificates involves validating the Organisations named in the Certificate (the Subjects). This process involves AusCERT or Participant Organisation RA, automatically or manually, reviewing and verifying the application information provided by the Applicant (as per section 4.1 of this CPS) in order to check that:

1. The Applicant has the right to use the domain name used in the application.
 - Validated by reviewing business name, or domain name ownership records or (for government and educational institutions associated with education and government domains only) receiving a letter on official departmental letterhead, with the order details and a statement verifying that the signor (which must be a WHOIS contact or senior member of management) is authorised to act on behalf of the Organisation. This process will be done when a new Participant Organisation signs an agreement with AusCERT and provides a list of domains owned by their Organisation. Such domains are included in the pre-validated domain list, not requiring subsequent validation unless the Participant Organisation changes these domains or asks for new ones to be included.
 - Validation may be supplemented through the use of the administrator contact associated with the domain name register record for communication with AusCERT validation staff or for automated email challenges.
 - Validation may be supplemented through the use of generic emails which ordinarily are only available to the person(s) controlling the domain name administration, for example webmaster@..., postmaster@..., admin@...
2. The Applicant is an accountable legal entity, whether an Organisation or an individual.
 - Validated by requesting official company documentation, such as Business License, Business Name, Articles of Incorporation, Sales License, ASIC company extract (or equivalent in jurisdictions outside Australia) or other documents held by ASIC (or equivalent body in jurisdictions outside Australia) or other relevant documents.
 - For non-corporate (including individual, government, and educational entities) applications, documentation such as partnership agreements, bank statement, copy of passport, copy of driving license or other relevant documents.

The above assertions are reviewed through an automated process, manual review of supporting documentation and reference to third party official databases.

4.2.1.2. Personal/Client Validated Certificate Validation

Validation of Personal Validated Certificates involves validating the identity of the individual requesting the Certificate. This process involves AusCERT or Participant Organisation RA, automatically or manually, reviewing the application information provided by the Applicant (as per section 4.1 of this CPS) in order to validate the identity of the Applicant and confirm that the email address is associated with the Applicant within an authorised domain of the Participant Organisation.

4.2.1.2.1. Standard Personal/Client Validated Certificate

Validated by reviewing that the Applicant is an entity of the Participant Organisation and has been recorded in the Organisations records database.

4.2.1.2.2. High Personal/Client Validated Certificate

Validated by confirming that the Applicant has provided proof of identity in person to the Participant Organisation's agents or Justice of Peace and accrues at least 100 points in accordance to the Financial Transaction Reports Act 1988 (FTR Act), Identification Record for a Signatory to an Account, '100 Point Check' Special Provisions (202) (www.austrac.gov.au/files/201_point_check.pdf).

4.2.1.3. Code Signing Certificate Validation

Code Signing Certificates are processed by AusCERT or the Participant Organisation in accordance with the process outlined for Organisation validated Certificates (4.2.1.1) and for high personal/client validated Certificates (4.2.1.2.2). AusCERT or the Participant Organisation may employ the data held in its domain databases to expedite the validation process. If the application data matches the records held by the Participant Organisation, manual validation intervention is not required.

4.2.2. Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a Certificate application, AusCERT or Participant Organisation RA will approve an application for a Certificate and AusCERT or Participant Organisation through the Certificate Services Manager web provisioning interface or any other mechanism made available by AusCERT will issue the Certificate.

If the validation of a Certificate application fails, AusCERT or Participant Organisation RA will reject the Certificate application. AusCERT reserves its right to reject applications to issue a Certificate to Applicants in its absolute discretion, including in circumstances where, on its own assessment, by issuing a Certificate to such parties the good and trusted name of AusCERT might get tarnished, diminished, or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such rejection.

Applicants whose applications have been rejected may subsequently re-apply.

The private key associated with a public key, which has been submitted as part of a rejected Certificate application, may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected Certificate. The private key may also not be resubmitted as part of any other Certificate application.

4.2.3. Time to Process Certificate Applications

Reasonable efforts are made to confirm Certificate application information and issue a Certificate within a reasonable time frame. The time frame is greatly dependent on the Applicant providing the necessary details and / or documentation in a timely manner. Upon the receipt of the necessary details and / or documentation, AusCERT or Participant Organisation RA aims to confirm submitted application data and to complete the validation process and issue / reject a Certificate application within two (2) working days.

From time to time, events outside of the control of AusCERT may delay the issuance process. However AusCERT will make every reasonable effort to meet issuance times and to make Applicants aware of any factors that may affect issuance times in a timely manner.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

AusCERT or Participant Organisation issues a Certificate upon approval of a Certificate application or upon request of a Certificate from a previously validated Participant Organisation. A Certificate is deemed to be valid at the moment a Subscriber accepts it (refer to section 4.4 of this CPS). Issuing a Certificate means that AusCERT accepts a Certificate application.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

AusCERT notifies the Subscriber and/or Participant Organisation of the issuance of a Certificate within a reasonable amount of time after the Certificate is created. Issued Certificates may either be downloaded by the Subscriber or Participant Organisation or may be installed by AusCERT directly (depending on the Certificate type).

4.3.3. Notification of Certificate Issuance by the CA to Other Entities

Other parties involved in the issuance and approval of the Certificate may receive notification of the issuance of a Certificate to their customer or client.

4.4. Certificate Acceptance

An issued Certificate is either delivered via email or installed on a Subscriber's computer / hardware security module through an online collection method.

4.4.1. Conduct Constituting Certificate Acceptance

A Subscriber is deemed to have accepted a Certificate when:

- the Subscriber uses the Certificate, or
- 30 days pass from the date of the issuance of a Certificate

4.4.2. Publication of the Certificate by the CA

An issued Certificate is published by delivering the Certificate to the Subscriber. Participant Organisations may choose to publish at their own discretion Certificates issued to their entities.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Participant Organisations must ensure a Subscriber has agreed to a Subscriber Agreement before it uses a private key.

Use of the private key is prohibited until the Subscriber has agreed to a Subscriber Agreement. Certificates may only be used for lawful and appropriate purposes as set forth in this CPS. Subscribers are responsible for protecting their private keys from unauthorised use and agree to take all reasonable steps to prevent unauthorised use of their private key and immediately cease using the Certificate following the expiration or revocation of the Certificate.

4.5.2. Relying Party Public Key and Certificate Usage

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the Relying Party. Reliance on a digital signature should only occur if:

- the digital signature was created during the operational period of a valid Certificate and it can be verified by referencing a validated Certificate;
- the Relying Party has checked the revocation status of the Certificate by referring to the relevant OCSP and the Certificate has not been revoked;
- the Relying Party understands that a Certificate is issued to a Subscriber for a specific purpose and that the private key associated with the Certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the Certificate profile; and
- the Certificate applied for is appropriate for the application it is used in.

Reliance is accepted as reasonable under the provisions made for the Relying Party under this CPS and within the Relying Party Agreement. If the circumstances of reliance exceed the assurances delivered by AusCERT under the provisions made in this CPS, the Relying Party must obtain additional assurances on its own.

Any warranties are only valid if the steps detailed above have been carried out.

4.6. Certificate Renewal

Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

Renewal fees, if applicable, are detailed on the official AusCERT websites and within communications sent to Subscribers approaching the Certificate expiration date. AusCERT and/or Participant Organisation shall make reasonable efforts to notify Subscribers via e-mail of the imminent expiration of a Certificate. Notice, unless stipulated otherwise by the Participant Organisation, shall ordinarily be provided within a 60-day period prior to the expiration of the Certificate.

4.6.1. Circumstances for Certificate Renewal

A Subscriber may renew an existing Certificate prior to or after its expiration by submitting a renewal request on line or in writing to AusCERT or Participant Organisation.

4.6.2. Who May Request Renewal

The Subscriber of the Certificate or an authorised representative must be the party requesting the Certificate's renewal.

4.6.3. Processing Certificate Renewal Requests

Renewal applications and requests undergo the same identity check as detailed for new customers.

4.6.4. Notification of New Certificate Issuance to Subscriber

Notification of a new Certificate issuance is performed in accordance with Section 4.3.3.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting acceptance of a renewed Certificate is the same as specified in Section 4.4.1.

4.6.6. Publication of the Renewal Certificate by the CA

A renewed Certificate is published as specified in Section 4.4.2.

4.6.7. Notification of Certificate Issuance by the CA to other Entities

A Participant Organisation may receive notification of its customer's Certificate renewal.

4.7. Certificate Re-key

AusCERT does not support Certificate re-key.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

Certificate information may change during the life of the Certificate. In this case, AusCERT will issue a new Certificate based on the new information properly notified to AusCERT rather than modifying an existing Certificate. Certificate modification is considered and handled the same as an application for a new Certificate.

4.8.2. Who May Request Certificate Modification

See 4.1.1.

4.8.3. Processing Certificate Modification Requests

See 4.1.2.

4.8.4. Notification of New Certificate Issuance to Subscriber

See 4.3.2

4.8.5. Conduct Constituting Acceptance of Modified Certificate

See 4.4.1

4.8.6. Publication of the Modified Certificate by the CA

See 4.4.2.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

See 4.4.3

4.9. Certificate Revocation and Suspension

Upon revocation of a Certificate, the operational period of that Certificate is immediately considered terminated. The serial number of the revoked Certificate will be placed on the next published CRL and be displayed as revoked from within the OCSP. The Certificate's listing on the CRL will remain until after the end of the Certificate's validity period.

4.9.1. Circumstances for Revocation

Revocation of a Certificate is the permanent end of the operational period of the Certificate prior to reaching the conclusion of its stated validity period. AusCERT may revoke a Certificate if any of the following occur:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key associated with the Certificate;
- The Subscriber or AusCERT has breached a material obligation under this CPS or the relevant Subscriber Agreement;
- Either the Subscriber's or AusCERT's obligations under this CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- There has been a modification of the information pertaining to the Subscriber that is contained within the Certificate;
- A personal identification number, private key or password has, or is likely to become known to someone not authorised to use it, or is being or is likely to be used in an unauthorised way;
- A Subscriber's Certificate has not been issued in accordance with the policies set out in this CPS;
- The Subscriber has used the subscription service referred to in this CPS contrary to law, rule or regulation, AusCERT or Participant Organisation reasonably believes that the Subscriber is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Certificate is being used or is suspected to be used to distribute or sign malware;
- The information contained in the Certificate is incorrect or has changed;
- The Certificate was issued as a result of fraud or negligence; or
- The Certificate, if not revoked, may compromise the trust status of AusCERT.
- AusCERT receives a complaint in relation to the Certificate or a request that the Certificate be revoked.

When considering whether or not the Certificate should be revoked, AusCERT will consider:

- The nature and number of complaints received
- The nature of the complaining party
- Relevant legislation and industry standards
- Additional outside input regarding the trust status of the Certificate or the nature of the use of the Certificate

4.9.2. Who can Request Revocation

The Subscriber, Participant Organisation or other appropriately authorised parties can request revocation of a Certificate. Prior to the revocation of a Certificate on the basis of such a request, AusCERT or the Participant Organisation RA will verify that the revocation request has been made by the Organisation or individual entity that has made the Certificate application. AusCERT has a unilateral right to revoke a Certificate, including on the basis of a third party notification or request.

4.9.3. Procedure for Revocation Request

Generally, Participant Organisations, through their RAs, are responsible for accepting and rejecting revocation requests within their own domain. However, AusCERT retains the ability to control the entire Certificate lifecycle and may process revocation requests in its sole discretion. The following procedure is used to authenticate a revocation request sent to AusCERT:

- The revocation request must be sent by the administrator contact associated with the Certificate application. AusCERT may, if necessary, also request that the revocation request be made by either the Participant Organisation RA, Organisational contact or the billing contact.
- Upon receipt of the revocation request, AusCERT or the Participant Organisation RA will request confirmation from the known administrator out of bands contact details, either by telephone, signed email or by fax.
- AusCERT or Participant Organisation validation personnel will then command the revocation of the Certificate using the Certificate Services Manager web provisioning interface or any other mechanism made available by AusCERT. The reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

4.9.4. Revocation Request Grace Period

There is no revocation grace period.

4.9.5. Revocation Checking Requirement for Relying Parties

Relying Parties must always check the status of the Certificate on which they are relying. Relying Parties may check the OCSP and/or CRL or use the applicable web-based AusCERT Repository to confirm that the Certificate has not been revoked or expired.

4.9.6. Time Within Which CA Must Process the Revocation Request

AusCERT or Participant Organisation processes all revocation requests without delay. The amount of time required depends on the nature of the revocation request, the party requesting the revocation, and other factors surrounding the revocation request. AusCERT will revoke the Certificate and place the Certificate in the OCSP and/or CRL once it has determined, to AusCERT's satisfaction, that the revocation request was proper.

4.9.7. CRL Issuance Frequency

An updated CRL is published on the AusCERT Repository by Comodo automated system every 24 hours. Under special circumstances the CRL may be published more frequently.

4.9.8. Maximum Latency for CRLs

CRLs are posted to the online AusCERT Repository within a commercially reasonable time after their generation. Usually, this is within a minute of the CRL's generation.

4.9.9. On-line Revocation/Status Checking Availability

AusCERT through Comodo's automated system manages and makes publicly available directories of revoked Certificates using Certificate Revocation Lists (CRLs). All CRLs issued by AusCERT are X.509v2 CRLs as profiled in RFC3280. Users and Relying Parties are strongly urged to consult the directories of revoked Certificates at all times prior to relying on information featured in a Certificate. AusCERT updates and publishes a new CRL every 24 hours or more frequently under special circumstances. The CRL for end entity Certificates can be accessed via crl.cs.auscert.org.au.

4.9.10. On-line Revocation Checking Requirements

Relying Parties must confirm the validity of a Certificate via the CRL prior to relying on the Certificate.

4.9.11. Other Forms for Revocation Advertisements available

Not applicable.

4.9.12. Special Requirements Re-key Compromise

Not applicable.

4.9.13. Circumstances for Suspension

AusCERT does not utilise Certificate suspension.

4.9.14. Who can Request Suspension

Not applicable

4.9.15. Procedure for Suspension Request

Not applicable

4.9.16. Limits on Suspension Period

Not applicable

4.10. Certificate Status Services

4.10.1. Operational Characteristics

AusCERT utilises both CRLs and an OCSP to allow Relying Parties to verify the validity of a Certificate. Each CRL and the OCSP contain information for all of AusCERT's revoked or un-expired Certificates.

Each CRL contains entries for all revoked un-expired Certificates issued and is valid for 24 hours. Comodo on behalf of AusCERT issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, AusCERT may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in Section 5.5 of this CPS) for a period of 7 years or longer if applicable.

Individual entries into the OCSP can be requested using the AusCERT OCSP responder. Revoked Certificates are affected in the OCSP within 24 hours after their revocation.

4.10.2. Service Availability

The OSPP provides access to Certificate status information 24x7. CRL's are open to public inspection 24x7.

4.10.3. Optional Features

Not applicable.

4.11. End of Subscription

A Subscriber may terminate a subscription to AusCERT's Certificate services by allowing the Certificate to expire without renewal or by requesting that AusCERT or Participant Organisation RA revoke the issued Certificate.

Participant Organisations can terminate their agreement with AusCERT providing 30 days' notice in writing to AusCERT and by revoking all Certificates issued to the Participant Organisation.

4.12. Key Escrow and Recovery

Subscribers are solely responsible for protection of their private keys and are encouraged to keep a backup of their private key as per their Participant Organisation policies.

However, the AusCERT Certificate Services Manager maintained by Comodo may back up the private keys it generates and protects such keys by encrypting them and storing them on a secure server on behalf of the Participant Organisation. This process only occurs if agreed by AusCERT and requested by the Participant Organisation at time of joining this service or at any time that key escrow is enabled by the Participant Organisation. If requested by the Participant Organisation RA, under special circumstances the keys can be recovered and decrypted by either the Certificate Subscriber, the Participant Organisation which ordered the Certificate or AusCERT/Comodo.

AusCERT may charge a fee to perform key escrow and recovery for the Participant Organisation.

Private keys are delivered in passphrase protected PKCS#12 format to the authorised requestor via email. The passphrase that protects the delivered private key is selected by the account administrator who can communicate this to the authorised requestor via an alternative channel.

Escrowed private keys are kept by Comodo on behalf of AusCERT for five years prior to their destruction. Private keys are destroyed by deleting the key from the storage material plus deleting all related back up material.

Subscribers should use a password or equivalent authentication method, and suitable access controls to prevent unauthorised access to and usage of the Subscriber private key.

See Section 6.2.3 of this CPS for more details on private key escrow.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Security Controls

AusCERT's CA infrastructure is hosted by Comodo on a secure site to prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

5.1.1. Site Location and Construction

The Comodo data center housing the AusCERT PKI Certificate Services is operated under a secure policy to ensure that no unauthorised logical or physical access is allowed.

Most records are archived at a secure off-site location and are maintained in a form that prevents unauthorised modification, substitution or destruction.

5.1.2. Physical Access

Access to facilities is limited to Comodo personnel using physical access control and is only accessible to appropriately authorised individuals (referred to hereon as "Trusted Personnel"). Card access systems are in place to control, monitor and log access to all areas of the facility. Access to physical machinery within the secure facility is protected with locked cabinets and logical access control.

5.1.3. Power and Air Conditioning

Facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

5.1.4. Water Exposures

Comodo has taken reasonable steps to ensure that the AusCERT CA system is secure and protected from flood and water damage.

5.1.5. Fire Prevention and Protection

Fire protection and prevention is made in compliance with local fire regulations in UK.

5.1.6. Media Storage

All media storing AusCERT data or information, including media containing audit logs, archived records, software, Subscriber information, and other information pertinent to the AusCERT CA's operation is

stored by Comodo in a secure facility that has implemented both logical and physical controls that limit potential harm to the data.

5.1.7. Waste Disposal

Sensitive documents are shredded prior to disposal. Electronic media is wiped clean by a trusted source upon the expiration of the data. All media is rendered unreadable prior to its disposal and, where possible, is physically destroyed. Comodo, AusCERT and Participant Organisations, where applicable must observe this procedure.

5.1.8. Off-site Backup

Routine AusCERT CA infrastructure backups of all sensitive information are stored by Comodo in accordance to Comodo's policies in a separate secure location using a third party data center.

5.2. Procedural Controls

5.2.1. Trusted Personnel

Trusted Personnel are parties allowed to access the AusCERT account management system; these can be staff from Comodo, AusCERT or Participant Organisations. Persons acting as Trusted Personnel are granted functional permissions to the account management system. All permissions are applied on an individual basis and are decided by senior members of AusCERT management team. All signed authorizations are archived.

5.2.2. Personnel Controls

All personnel assigned to validation are appointed by AusCERT or the Participant Organisation; these must be trustworthy staff and are allowed to validate Certificate requests. Personnel are trained on the validation processes found herein prior to assisting in any validation.

5.2.3. Identification and Authentication for Trusted Personnel

Trusted Personnel must identify and authenticate themselves before system access is granted. Identification is either via a username and password, or username and password and additional Certificate authentication, if 2 factor authentication is preferred.

5.2.4. Personnel Responsibilities

Participant Organisation RAs are responsible for

- Validation of Certificate Applications and renewals on behalf of their Organisations
- Approval or rejection of Certificate Applications on behalf of their Organisations

AusCERT personnel are responsible for

- Approval or rejection of Certificate Applications
- Certificate Issuance and Revocations
- Invoking tools that enable the use of the CA key
- At AusCERT's discretion, validation of Certificate Applications

Comodo personnel are responsible for

- Management of the CA key, including issuance or destruction of a CA Certificate
- Management of AusCERT CA infrastructure.

5.3. Personnel Security Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

Comodo, AusCERT and RAs follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory

performance of their duties. Personnel performing validation functions must have the necessary qualifications or experience to follow the required process.

5.3.2. Training Requirements

Personnel's training occurs via a mentoring process involving senior members of the team to which the employee is attached. All training programs are periodically reviewed and enhanced as necessary.

Training programs are tailored toward each individual's job responsibilities and may include training on PKI concepts, job responsibilities, operational policies and procedures, incident handling and reporting, and disaster recovery procedures.

5.3.3. Retraining Frequency and Requirements

Refresher training courses are provided to personnel in order to ensure that all such personnel can competently and satisfactorily perform their job responsibilities.

5.3.4. Job Rotation Frequency and Sequence

No Stipulation

5.3.5. Sanctions for Unauthorised Actions

Any personnel found violating a policy or procedure described in this CPS is subject to disciplinary action. The action taken by Comodo, AusCERT and Participant Organisation depends on the circumstances surrounding the action, the severity of the violation, and the personnel's past performance. In some cases, disciplinary action may include the personnel's termination.

5.3.6. Independent Contractor Requirements

If an independent contractor or consultant is used, Comodo, AusCERT and Participant Organisation shall first ensure that each such contractor or consultant is first obligated to abide by the same functional and security criteria that are set forth herein. Contractors and consultants are subject to the same sanctions as other personnel as set forth in Section 5.3.5.

5.3.7. Documentation Supplied to Personnel

All personnel are supplied with the training and documentation needed to perform their job responsibilities. Personnel understand and are obligated and required to safe guard and protect all private and confidential information to which they might have access.

5.4. Audit Logging Procedures

Electronic or manual logs of the following events for core functions listed in Section 5.4 are retained by Comodo.

5.4.1. Types of Events Recoded

CA & Certificate Lifecycle Management

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber Certificate life cycle management, including successful and unsuccessful Certificate applications, Certificate issuances, Certificate re-issuances and Certificate renewals
- Subscriber Certificate revocation requests, including the reason for the revocation
- Subscriber changes of affiliation that would invalidate the validity of an existing Certificate
- Certificate Revocation List updates, generations and issuances
- OCSP updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a private key

Security Related Events

- System downtime, software crashes, and hardware failures
- CA system actions, including software updates, hardware replacements, and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service, or repair and retirement
- Successful and unsuccessful AusCERT CA infrastructure access attempts
- Secure CA facility visitor entry and exit

An audit log is maintained of each movement of the removable media.

Certificate application information retained by Comodo, AusCERT or Participant Organisation:

- The documentation and other related information presented by the Applicant as part of the application validation process
- Storage locations, whether physical or electronic, of presented documents

5.4.2. Frequency of Processing Log

Logs are review on a weekly basis by AusCERT CA management.

5.4.3. Retention Period of Audit Log

Logs are archived by Comodo's system administrator on a weekly basis by the system administrator. Logs are thereafter retain as part of the record archive as set forth in Section 5.5.

5.4.4. Protection of Audit Log

All logs are backed up by Comodo on removable media and the media held at a secure off-site location on a daily basis. These media are only removed by Comodo staff or AusCERT staff on a visit to the data centre, and when not in the data centre are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

5.4.5. Audit Log Backup Procedures

Logs are archived by Comodo's system administrator on a weekly basis. Both current and archived logs are maintained in a form that prevents unauthorised modification, substitution or destruction. When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the Certificates of destruction are archived.

5.4.6. Audit Collection System

Audit data is generated both automatically and manually. All logs generated by Comodo include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

5.4.7. Notification to Event-Causing Subject

Notice of audited events are confidential information and AusCERT is not obliged to give notice to individuals or Organisations unless required by law or agreement.

5.4.8. Vulnerability Assessments

Events in the audit process are logged to monitor vulnerabilities. Security procedures and updates are periodically reevaluated as required.

5.5. Records archival

5.5.1. Types of records archived

The following information may be archived:

- Information or documentation submitted by Subscribers in support of a Certificate application to Participant Organisation, AusCERT or Comodo.
- Copies of Certificates, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that AusCERT or Comodo may see fit.
- Participant Organisations must keep records of their assigned RAs and any related documentation.
- Audit logs
- Other records deemed important and valuable to AusCERT's business operations.

5.5.2. Retention period for archive

Records of AusCERT Certificates and the associated documentation is retained for a term of 7 years after the expiration of the Certificate, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation.

5.5.3. Protection of archive

Records are archived at a secure location and are maintained in a form that prevents unauthorised modification, substitution or destruction.

5.5.4. Archive backup procedures

Electronic archives are regularly backed up by Comodo and copies are maintained of paper files.

5.5.5. Requirements for time-stamping of records

Certificates, CRLs, and other archived information shall contain time and date information that may or may not be cryptographic-based.

5.5.6. Archive collection system

The Comodo archive collection system is a private system.

5.5.7. Procedures to obtain and verify archive information

Only AusCERT and Comodo authorised Trusted Personnel are permitted access to the archive. Subscribers may obtain copies of archived information related to their Certificates upon written request and payment of any associated costs. Subject to compliance with applicable laws, access to such information is at AusCERT's or the relevant holder of the information's discretion.

5.6. Key changeover

Towards the end of each private key's lifetime, a new CA signing key pair is commissioned by Comodo and all subsequently issued Certificates are signed with the new private signing key. Both keys may be concurrently active. The corresponding new CA public key Certificate is provided to Subscribers and Relying Parties through the delivery methods detailed in Section 6.1 of this CPS.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

To maintain AusCERT CA operations when an incident occurs, Comodo makes a backup of critical CA software weekly and is stored offsite. Backups of critical business information are performed daily and are stored offsite. Further, operations are distributed across several sites worldwide. All sites offer facilities to manage the lifecycle of a Certificate, including but not limited to the application, issuance, revocation and renewal of such Certificates.

5.7.2. Computing resources, software, and/or data are corrupted

A backup CA is readily available from Comodo in the event that the primary AusCERT CA should cease operation. All critical computer equipment is housed in a co-location facility run by a commercial data-

centre, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated.

In addition, a backup AusCERT CA and a secondary site can be activated should the primary site suffer a total loss of systems. The Comodo disaster recovery plan endeavors to minimize interruptions to CA operations.

5.7.3. Business continuity capabilities after a disaster

Comodo's disaster recovery plans and procedures are maintained, tested, and periodically updated to ensure the integrity of its systems. Such plans are revised and updated as may be required at least once a year.

5.8. CA termination

In the event that it is necessary for AusCERT to cease CA operation, AusCERT shall make a commercially reasonable effort to notify Participant Organisations of such termination in advance of the effective date of the termination. Should AusCERT cease its CA operations, AusCERT shall develop a termination plan to minimize the disruption of services to Subscribers. The plan shall provide for:

- Revocation of Certificates issued to the CA
- Revocation of unexpired and unrevoked Certificates issued by AusCERT CA as may be necessary
- Preservation of the CA's archives and records as required by this CPS
- Disposition of the CA's private key

6. TECHNICAL SECURITY CONTROLS

The AusCERT CA infrastructure is hosted and operated by Comodo in accordance to Comodo's security controls and policies.

Comodo's operational sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorised logical or physical access to CA related facilities. This section of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

6.1. Key pair generation and installation

6.1.1. Key pair generation

AusCERT CA Root private key(s) are secured and protected using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4). Necessary precautions are taken to prevent the compromise or unauthorised usage of the keys.

The AusCERT CA Root key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

The Subscriber is solely responsible for the generation of the private key used in the Certificate signing request. AusCERT provides key generation along with escrow, recovery, and backup services for private keys generated on Comodo's servers. Keys are generated during the ordering process for the Certificate on Comodo's servers and then delivered to Subscriber through the Internet. Comodo server generated private keys may be retrieved by entering a password.

Upon making a Certificate application, the Subscriber is responsible for the generation of an RSA key pair appropriate to the Certificate type being applied for (which may be generated by AusCERT or Participant Organisation on Subscriber's behalf). During application, the Subscriber will be required to submit a public key and other personal / corporate details in the form of a Certificate Signing Request (CSR).

SSL Certificate requests are generated using the key generation facilities available in the Subscriber's webserver software.

6.1.2. Certificate and Certificate Chain delivery to Subscriber

AusCERT provides the full Certificate chain to the Subscriber upon issuance and delivery of the Subscriber Certificate.

AusCERT incorporates by reference the following information in every Certificate it issues:

- Terms and conditions of the Certificate.
- Any other applicable Certificate policy as may be stated on an issued AusCERT Certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customised elements of the standard X.509v3.
- Content of extensions and enhanced naming that are not fully expressed within a Certificate.
- Any other information that is indicated to be so in a field of a Certificate.

Delivery of Subscriber Certificates to the associated Subscriber is dependent on the Certificate product type:

6.1.2.1. Server Certificate

If AusCERT's domain databases hold sufficient validation information, an automatic validation of the Certificate Application may take place. In the event of such an automated validation the Certificate is delivered to commonly used generic email addresses ordinarily belonging to authorised personnel at the domain name used in the application, such as webmaster@... admin@... postmaster@... hostmaster@..., in addition to the master RA within the Organisation, or placed in the website advised by AusCERT. Confirmation of the Certificate delivery location is provided to the administrator contact provided during the application process. If the Certificate is validated outside of AusCERT's databases, then the secure server Certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

6.1.2.2. Delivery of other Certificates

Unless otherwise specified through an amendment to this CPS, all other Certificates shall be delivered to the relevant party through email using a Subscriber-provided email address or placed at the website advised by AusCERT for pick up.

6.1.3. Public key delivery to Certificate issuer

Server Certificate requests are generated using the Subscriber's software and the request is submitted to AusCERT in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via the AusCERT website or through an AusCERT approved RA.

6.1.4. CA public key delivery to Relying Parties

AusCERT makes all its CA Root Certificates available in the online AusCERT Repository at cs.auscert.org.au/repository/.

The UTN USERFirst Hardware Certificate is present in Explorer 5.01 and above, Netscape 8.1 and above, Opera 8.0 and above, Mozilla 1.76 and above, Konqueror 3.5.2 and above, Safari 1.2 and above, FireFox 1.02 and above, Camino and SeaMonkey and is made available through these browsers.

The AddTrust External CA Root Certificate is present in Netscape 4.x and above, Opera 8.00 and above, Mozilla .06 and above, Konqueror, Safari 1.0 and above, Camino and SeaMonkey and is made available to Relying Parties through these browsers.

6.1.5. Key sizes

Key pairs are of sufficient length to prevent unauthorised determination or reverse engineering of the private key. Most keys are 2048 bit keys; however some 1024 bit intermediate keys exist. See Appendix A for the size of each issued key.

6.1.6. Public key parameters generation and quality checking

The AusCERT private key(s) are generated and secured using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), and takes necessary precautions to prevent the compromise or unauthorised usage of them.

The AusCERT CA Root key was generated in accordance with the guidelines detailed in the Comodo Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

The key usage field extension in AusCERT Certificates specifies the purpose for which the Certificate may be used. Enforcement of the limitations of use found in this field is beyond AusCERT's control as its correct use is highly dependent on having the correct software.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

AusCERT CA Root key pairs are protected in accordance with this CPS.

6.2.1. Cryptographic module standards and controls

Comodo protects the UTN and AddTrust CA Root key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Comodo's WebTrust compliancy are available at its official website (www.comodogroup.com).

AusCERT private keys are generated and store on an IBM 4758 accredited to FIPS PUB 140-1 level 4 by Comodo.

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

For AusCERT CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment. The decryption key is split across **5** removable media and requires **3 of 5** to reconstruct the decryption key. Custodians in the form of two or more authorised Comodo and/or AusCERT officers are required to physically retrieve the removable media from the distributed physically secure locations.

6.2.3. Private key escrow

A Subscriber with an escrowed private key may only recover the key upon confirmation of the identity of the party requesting the private key and upon a request from the Participant Organisation. This identity is checked by having the user enter a unique password and user name or any other mechanism defined by AusCERT and Participant Organisation. Participant Organisations may only escrow private keys for lawful and legitimate purposes. AusCERT requires Participant Organisation to notify their employees and others receiving a Certificate through their account if the related private keys are escrowed and that Subscribers should take reasonable steps to backup and protect their private key. Subscribers are not allowed to disclose any escrowed keys or escrowed-key related information to a third party unless required by law. Participant Organisation RAs are required to revoke the Certificate associated with an escrowed private key prior to retrieving the escrowed key.

6.2.4. Private key backup

AusCERT's CA keys are generated and stored inside cryptographic hardware by Comodo. The keys are backed up and transferred in an encrypted form.

The Subscriber is responsible for back up and protection of their private keys. AusCERT may provide key escrow and backup services for keys it generates as detailed in Section 6.2.3 at its discretion. AusCERT strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorised access and usage of the Subscriber private key.

6.2.5. Private key archival

When any AusCERT CA Root Signing Key pair expires, they will be archived by Comodo for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration by Comodo.

6.2.6. Private key transfer into or from a cryptographic module

Where AusCERT CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only by Comodo.

6.2.7. Private key storage on cryptographic module

AusCERT private keys are generated and stored on an IBM 4758 accredited to FIPS PUB 140-1 level 4 by Comodo.

6.2.8. Method of activating private key

AusCERT's private keys are activated according to the specifications of the cryptographic hardware manufacturer.

Subscribers are responsible for protecting their own private keys and should take commercially reasonable steps to prevent physical or logical unauthorised access to a private key.

6.2.9. Method of deactivating private key

All deactivated private keys should be kept in an encrypted form only. Keys are deactivated by logging off their system. Root keys are further deactivated by removing them from their storage partition.

6.2.10. Method of destroying private key

Private keys are destroyed by deleting them from all known storage partitions and then by zeroizing or by physically destroying the hardware on which they were stored. All AusCERT CA key destruction activities are logged by Comodo.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other aspects of key pair management

No Stipulation

6.3.1. Public key archival

Copies of all public keys are retained via a routine backup procedure as described in Section 5.5.

6.3.2. Certificate operational periods and key pair usage periods

The operational period of each Certificate generated ends upon its revocation or expiration. The operational period of each CA key is set forth in Appendix A.

The validity period of AusCERT Certificates varies depending on the Certificate type, but typically, a Certificate will be valid for 1 to 4 years. AusCERT reserves the right to, at its discretion, issue Certificates that may fall outside of these set periods.

6.4. Activation data

6.4.1. Activation data generation and installation

Cryptographic module containing private keys are activated according the specifications set forth by the hardware manufacture and meets the requirements of FIPS 140-2 Level 4. All cryptographic hardware used by Comodo to support the AusCERT Certificate service is under two-personnel control.

Personnel are required to use strong passwords (non-dictionary alphanumeric passwords with a minimum length that are changed on a regular basis) to protect sensitive information.

6.4.2. Activation data protection

Data is protected using strong passwords as described in Section 6.4.1.

6.4.3. Other aspects of activation data

All activation is transmitted, stored, and destroyed using methods and procedures protecting against loss, theft, modification, or any other unauthorised access, loss, or use.

6.5. Computer security controls

The CA Infrastructure is managed by Comodo which uses trustworthy systems to provide Certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

6.5.1. Specific computer security technical requirements

Comodo computer systems are set up and maintained in a secure manner that prevents unauthorized access. Comodo uses software and hardware that constitute the industry's best practice in security measures.

Computers are password protected and require a strong password for access. All passwords are changed on a regular basis. Computers are firewalled and scanned regularly for viruses, spyware, Trojans, and other malware.

6.5.2. Computer security rating

No Stipulation.

6.6. Life cycle technical controls

6.6.1. System development controls

All systems and software are developed and implemented in accordance with industry standards. All systems and software are routinely checked for malware and security issues by Comodo.

6.6.2. Security management controls

Changes in Security-related changes are logged and processed by Comodo. Security policies and controls are periodically reviewed and updated to ensure that no unauthorized access is allowed.

6.6.3. Life cycle security controls

No Stipulation.

6.7. Network security controls

All AusCERT CA functions are performed on secured networks to prevent unauthorized access and other malicious activity.

6.8. Time-stamping

Certificates, CRLs, and OCSP entries generated by Comodo shall contain time and date information about the Certificate, CRL, or OCSP information. Such information may not be cryptographic based.

7. CERTIFICATE, CRL, AND OCSP PROFILES

AusCERT currently offers a portfolio of Certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications.

AusCERT offers a range of distinct Certificate types. The different Certificate types have differing intended usages and differing policies.

As the suggested usage for a Certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific Certificate.

AusCERT may update or extend its list of products, including the types of Certificates it issues, as it sees fit and shall not be subject to claims by any party as a result of changes to such lists. If necessary,

AusCERT shall amend this CPS upon the inclusion of a new Certificate product in the AusCERT PKI hierarchy. The CPS shall usually be made public on the official AusCERT websites at least seven (7) days prior to the offering such new product.

Revoked Certificates are appropriately referenced in the CRL and/or OCSP.

7.1. Certificate profile

AusCERT OV Certificates may not be used for Monetary Transactions. In order to use and rely on an AusCERT Certificate, the Relying Party must use X.509v3 compliant software.

7.1.1. Version number(s)

All AusCERT Certificates are X.509 version 3 Certificates.

7.1.2. Certificate extensions

AusCERT uses the standard X.509, version 3 to construct Certificates. X.509v3 allows a CA to add certain Certificate extensions to the basic Certificate structure. AusCERT uses a number of Certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is the standard of the International Telecommunications Union for Certificates.

7.1.2.1. Key Usage Extension field

AusCERT Certificates include key usage extension fields to specify the purposes for which the Certificate may be used and to technically limit the functionality of the Certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of AusCERT. AusCERT assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards meet the requirements set out in this CPS. Comodo and AusCERT cannot warrant that any such user software will support and enforce the controls required by AusCERT. All software use is left to the user's sole discretion.

The possible key purposes identified by the X.509v3 standard are the following:

- a) Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity
- b) Non-repudiation, for verifying digital signatures used in providing a non-repudiation service which protects against the signing entity falsely denying some action (excluding Certificate or CRL signing, as in f) or g) below)
- c) Key encipherment, for enciphering keys or other security information, e.g. for key transport
- d) Data encipherment, for enciphering user data, but not keys or other security information as in c) above
- e) Key agreement, for use as a public key agreement key
- f) Key Certificate signing, for verifying a CA's signature on Certificates, used in CA Certificates only
- g) CRL signing, for verifying a CA's signature on CRLs.
- h) Encipher only, public key agreement key for use only in enciphering data when used with key agreement
- i) Decipher only, public key agreement key for use only in deciphering data when used with key agreement

7.1.2.2. Extension Criticality Field

The Extension Criticality field denotes two separate uses for the Key Usage field. If the extension is noted as critical, then the key in the Certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, the Key Usage field is simply there as an aid to help applications find the proper key for a particular use.

7.1.2.3. Basic Constraints Extension

The Basic Constraints extension specifies whether the Subject of the Certificate may act as a CA or only as an end-entity. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of AusCERT.

7.1.3. Algorithm object identifiers

AusCERT uses the UTN-USERFIRST-Hardware, AddTrust External, UTN-DataCorp SGC Root, UTN-UserFirst-Client Authentication and Email Root and UTN-UserFirst-Object Root for its Root CA Certificates. This allows AusCERT to issue highly trusted Certificates by inheriting the trust level associated with the UTN root Certificate (named “UTN-USERFIRST-Hardware”) and the AddTrust root Certificate (named “AddTrust External CA Root”). The high-level representation of the AusCERT PKI set forth in Appendix C is used to illustrate the hierarchy utilised.

7.1.4. Name forms

AusCERT Certificates follow the naming policy set forth in Section 3.1.1.

7.1.5. Name constraints

No Stipulation

7.1.6. Certificate policy object identifier

Certificate Policy (“CP”) is a statement of the issuer that corresponds to the prescribed usage of a Certificate within an issuance context. A policy identifier is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a Certificate policy.

Specific AusCERT Certificate profiles are provided in Appendix D.

7.1.7. Usage of Policy Constraints extension

No Stipulation

7.1.8. Policy qualifiers syntax and semantics

AusCERT usually includes information in the Policy Qualifier field of the Certificate Policy extension that puts Relying Parties on notice of the location of its CPS. This field usually includes a URL that points the Relying Party to the CPS where they can find out more about the limitations on liability and other terms and conditions governing the use of the Certificate. The lack of such information does not mean the CPS does not apply.

7.1.9. Processing semantics for the critical Certificate Policies extension

No Stipulation.

7.2. CRL profile

AusCERT manages and makes publicly available directories of revoked Certificates using Certificate Revocation Lists (CRLs) via Comodo automated tools. All CRLs issued by AusCERT are X.509v2 CRLs, in particular as profiled in RFC3280.

7.2.1. Version number(s)

CRLs conform to RFC 3280 and contain the basic fields listed below:

Version	[Version 2]	
Issuer Name	[Subject DN of the Issuer]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + 24 hours]	
Revoked Certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]
Authority Key Identifier	The identifier of Issuer’s public key	

CRL Number	Monotonically Increasing sequence number
-------------------	--

7.2.2. CRL and CRL entry extensions

No Stipulation.

7.3. OCSP profile

OCSP is way for users to obtain information about the revocation status of an AusCERT issued Certificate. AusCERT uses OCSP to provide information about all of its Certificates. OCSP responders conform to RFC 2560.

7.3.1. Version Number(s)

AusCERT uses Version 1 of the OCSP specification as defined by RFC2560.

7.3.2. OCSP Extensions

AusCERT's uses timestamp and validity periods to establish the accuracy of each OCSP response. Local time should be used by Participant Organisations to ensure the freshness of the OCSP response.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

8.1. Frequency or Circumstances of Assessment

An annual audit is performed by an independent external auditor to assess Comodo's compliancy with the AICPA/CICA WebTrust program for Certification Authorities.

8.2. Identity/Qualifications of Assessor

Audits are performed by a public accounting firm that:

- Is a highly reputable accredited accounting firm that is a member of the American Institute of Certified Public Accountants (AICPA)
- Has significant quality assurance mechanisms, including peer review, competency testing, and other measures.
- Abides by and conforms with the applicable standards and best practices as set forth by the relevant standards committees.
- Is knowledgeable about the operations of the CA and has an expertise in public key security technology, data centers, personnel controls, and other relevant fields of interest.
- Is knowledgeable about the operations of the CA and has an expertise in public key security technology.

8.3. Assessor's Relationship to Assessed Entity

The Assessor is independent of Comodo and AusCERT and does not have any financial interest or course of dealings with Comodo and AusCERT that could foreseeably create a significant bias in the Assessor's evaluation.

8.4. Topics Covered by Assessment

Topics covered by the annual audit include but are not limited to the following:

- CA business practices disclosure
- Service integrity
- CA environmental controls

8.5. Actions Taken as a Result of Deficiency

If any material noncompliance or deficiencies are discovered during an audit, then a plan is created and implemented to cure such deficiencies or noncompliance. In the event that the deficiency cannot be resolved, any Certificates affected by the deficiency or noncompliance will be revoked.

8.6. Communication of Results

No Stipulation

9. OTHER BUSINESS AND LEGAL MATTERS

This part of the CPS describes the business matters of AusCERT and legal representations, warranties and limitations associated with AusCERT Certificates. In the case of any inconsistency between this Section 9 and any other part of this CPS, the Section 9 shall prevail to the extent of any such inconsistency.

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

AusCERT may charge Participant Organisation fees and Subscriber fees for the Certificate services it offers, including issuance, and renewal. Fees are detailed on the official AusCERT websites (cs.auscert.org.au/repository/). AusCERT retains its right to change such fees from time to time.

9.1.2. Certificate Access Fees

Currently, AusCERT does not charge a fee for Certificate access, but reserves the right to establish and charge a reasonable fee for access to its database of Certificates. Charges may be incurred for extensive or time consuming searches. Fees for such extensive use are negotiated on an individual basis.

9.1.3. Revocation or Status Information Access Fees

AusCERT does not charge fees for the revocation of a Certificate or for a Relying Party to check the validity status of an AusCERT issued Certificate using its OCSP.

9.1.4. Fees for Other Services

Fees for other services offered by AusCERT are set either within the individual agreements with the parties or are detailed on the AusCERT Repository, depending on the services required. Fees may be discussed for other services by contacting AusCERT at:

AusCERT Certification Authority
AusCERT
The University of Queensland
QLD 4072
Australia

or by using the contact telephone numbers and addresses listed on the AusCERT Repository or AusCERT website at www.auscert.org.au.

9.1.5. Refund Policy

AusCERT is not obliged to refund any fees associated with a Certificate or any searches.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

No Stipulation

9.2.2. Other Assets

No Stipulation

9.2.3. Insurance or Warranty Coverage for End-Entities

AusCERT SSL Certificates may not be used for Monetary Transactions. As such, no Comodo Certificate warranty is associated with AusCERT's Certificates.

9.3. Confidentiality of Business Information

AusCERT observes applicable laws on the protection of confidential information. Comodo and Participant Organisations must also observe applicable laws on the protection of confidential information.

9.3.1. Scope of Confidential Information

AusCERT, Comodo and Participant Organisations, where applicable keep the following types of information confidential and maintain reasonable controls to prevent the exposure of such records to non-Trusted Personnel.

- Executed Subscriber Agreements.
- Certificate application records and documentation submitted in support of Certificate applications whether successful or rejected.
- Transaction records and financial audit records.
- External or internal audit trail records and reports
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of AusCERT infrastructure, Certificate management and enrolment services and data.

9.3.2. Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all Certificates issued by the AusCERT CA is public information. Subscriber application data marked as "Public" in the relevant Subscriber Agreement and submitted as part of a Certificate application is published within an issued Certificate in accordance with this CPS.

9.3.3. Responsibility to Protect Confidential Information

All AusCERT, Comodo and Participant Organisation personnel in trusted positions must handle all confidential information in strict confidence. Each party shall use the same degree of care that it exercises with respect to its own confidential information of like importance, but in no event shall the degree of care be less than a reasonable degree of care.

9.3.4. Disclosure Pursuant to Judicial or Administrative Process

AusCERT shall be entitled to disclose any confidential information as required by law or, if AusCERT believes, in good faith, that the disclosure is necessary in response to subpoenas, search warrants, right to information applications, or if disclosure is necessary in response to a pending legal proceeding.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

AusCERT observes applicable laws on the protection of personal information. Comodo and Participant Organisations must also observe applicable laws on the protection of personal information. The University of Queensland Privacy Policy (to which AusCERT is subject) can be found at: <http://www.uq.edu.au/hupp/index.html?page=24999>.

9.4.2. Information Treated as Private

Any personal information about Subscribers that is not publicly accessible or available through the content of the issued Certificate, a CRL, or the OCSP is treated as private information.

9.4.3. Information Not Deemed Private

Certificates, CRLs, the OCSP, and the information appearing in them are not considered private.

9.4.4. Responsibility to Protect Private Information

All AusCERT and Participant Organisation employees receiving private information are responsible to protect such information from compromise and disclosure to third parties. Each party shall use the same degree of care that it exercises with respect to its own information of like importance, but in no event shall the degree of care be less than a reasonable degree of care. In any case all parties shall comply with applicable privacy laws, including under the *Information Privacy Act 2009* (Qld).

9.4.5. Disclosure Pursuant to Judicial or Administrative Process

AusCERT shall be entitled to disclose any personal information as required by law or, if AusCERT believes, in good faith, that the disclosure is necessary in response to subpoenas and search warrants or if disclosure is necessary in response to a pending legal proceeding.

9.4.6. Other Information Disclosure Circumstances

No Stipulation.

9.5. Intellectual Property Rights

AusCERT or its partners or associates own all intellectual property rights associated with its databases, web sites, AusCERT Certificates and any other publication originating from AusCERT including this CPS.

9.5.1. Certificates

Certificates are the property of AusCERT. AusCERT gives permission to Participant Organisations and Subscribers to reproduce and distribute Certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full.

AusCERT shall retain and no other party shall obtain or claim any title or rights in (except as expressly licensed herein):

- (a) The Certificates and any other products referred to herein;
- (b) The techniques and ideas embedded in the Certificates or other products referred to herein;
- (c) Any copies and derivative works of the Certificates, software, related products or documentation or marketing material; or
- (d) Copyright, patent rights, trade secret rights or other proprietary rights in the Certificates or other products referred to herein.

AusCERT reserves the right to revoke the Certificate at any time. Private and public keys are property of the Subscribers who rightfully issue and hold them. All secret shares (distributed elements) of the AusCERT private key remain the property of AusCERT.

Participant Organisations and Subscribers each represent and warrant that when submitting to AusCERT and using a domain and distinguished name (and all other Certificate application information), they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to the third party's trademarks, service marks, trade names, company names, or any other intellectual property

right, and that the Participant Organisation or Subscriber is not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

9.5.2. Copyright

AusCERT owns the copyright in this CPS. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of AusCERT. Requests for any other permission to reproduce this AusCERT document (as well as requests for copies from AusCERT) must be addressed to:

cs@auscert.org.au

OR

AusCERT
The University of Queensland
QLD 4072
Australia

9.5.3. Trade marks

“AusCERT” is a trade mark of AusCERT and may only be used with permission of AusCERT.

AusCERT prohibits the use of a name or symbol that infringes upon the intellectual property rights of another. However, AusCERT does not verify or check the name appearing in a Certificate for non-infringement. Participant Organisations and Subscribers are solely responsible for ensuring the legality of any information presented for use in an AusCERT-issued Certificate.

Participant Organisations and Subscribers represent and warrant that when submitting an application to AusCERT and when using a domain and distinguished name (and all other Certificate application information) that they are not interfering with or infringing any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Although AusCERT will provide all reasonable assistance, Participant Organisations and Subscribers shall each defend, indemnify, and hold AusCERT harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of AusCERT.

AusCERT does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property or a domain's use of any infringing material. AusCERT, in its sole discretion and without any liability, may reject an application or revoke a Certificate, based on any intellectual property infringement claims or ownership disputes.

9.6. Representations and Warranties

Participant Organisations, Subscribers, Relying Parties and any other parties shall not interfere with or reverse engineer the technical implementation of AusCERT PKI services, including, but not limited to, the key generation process, the public web site, and the AusCERT repositories except as explicitly permitted by this CPS or upon prior written approval of AusCERT. Failure to comply with this as a Subscriber will result in the revocation of the Subscriber's Certificate without further notice to the

Subscriber. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the AusCERT Repository and any Certificate or service provided by AusCERT. AusCERT also reserves its rights to bring an action against any Participant Organisation, Subscriber, Relying Party or other party for such interference or reverse engineering.

Parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

9.6.1. CA Representations and Warranties

To the extent specified in the relevant sections of the CPS, AusCERT and Comodo, where applicable, each promise to:

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable Australian laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the AusCERT Repository and web site for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of Certificates that it may make publicly available.
- Issue Certificates in accordance with this CPS and fulfill its obligations presented herein.
- Publish accepted Certificates in accordance with this CPS.
- Provide support to Subscribers and Relying Parties as described in this CPS.
- Revoke Certificates according to this CPS.
- Provide for the expiration and renewal of Certificates according to this CPS.
- Make available a copy of this CPS and applicable policies to requesting parties.

Participant Organisations and Subscribers each acknowledge that neither AusCERT nor Comodo have any further obligations under this CPS.

AusCERT and Comodo disclaim all representations and warranties, either express or implied, by statute, general law, equity, international convention or custom, including, without limitation, warranties of merchantability, non-infringement, interoperability and fitness for a particular purpose, are disclaimed to the extent permitted by law.

AusCERT does not warrant the:

- accuracy, authenticity, completeness or fitness of any unverified information contained in Certificates or otherwise compiled, published, or disseminated by or on behalf of AusCERT except as it may be stated in the relevant product description below in this CPS and in the AusCERT insurance policy;
- quality, functions or performance of any software or hardware device; or
- validity, completeness or availability of directories of Certificates issued by a third party (including a Participant Organisation) unless specifically stated by AusCERT.

In addition, AusCERT shall not incur liability for representations of information contained in a Certificate except as it may be stated in the relevant product description in this CPS.

Although AusCERT is responsible for the revocation of a Certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.

Notwithstanding limitation warranties under the product section of this CPS, AusCERT shall not be responsible for non-verified subscriber information submitted to AusCERT, or the AusCERT directory or otherwise submitted with the intention to be included in a certificate.

9.6.2. Participant Organisation Representations and Warranties

Each Participant Organisation represents and warrants that it:

- Is part of the educational or research community of Australia, New Zealand, Fiji or Papua New Guinea.
- Has obtained and will obtain all necessary consents in respect of information included in its Certificate applications (including as required under the *Information Privacy Act 2009* (Qld)) and for use of the Certificate services.
- Has not and will not infringe any third party intellectual property rights in connection with its role in and use of the AusCERT PKI Certificate services.
- Will comply with this CPS and its internal or published policies and procedures.
- Will comply with applicable Australian and local laws and regulations.
- Will provide its Applicants with trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Will provide prompt notice in case of compromise of private key(s) within its Organisation.
- Will provide and validate application procedures for the various types of Certificates that it may use.
- Will issue Certificates in accordance with this CPS and fulfill its obligations presented herein.
- Will publish accepted Certificates in accordance with this CPS, if it publishes such Certificates.
- Will provide support to Subscribers and Relying Parties as described in this CPS.
- Will revoke Certificates according to this CPS.
- Will refer requests for copies of this CPS and applicable policies to the AusCERT Repository.

9.6.3. RA Representations and Warranties

AusCERT uses Participant Organisation RA's to validate and issue Certificates. Each RA represents and warrants that it will follow this CPS in validating Certificates prior to their issuance and in managing each Certificates lifecycle. RAs may not undertake any actions that might imperil, put in doubt or reduce the trust associated with the AusCERT products and services. Failure to comply with this will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the AusCERT Repository and any Certificate or Service provided by AusCERT.

9.6.4. Subscriber Representations and Warranties

Upon accepting a Certificate, the Subscriber represents and warrants to AusCERT and to Relying Parties that at the time of acceptance and until further notice:

- It is part of the educational or research community of Australia, New Zealand, Fiji or Papua New Guinea.
- It has obtained and will obtain all necessary consents in respect of information included in its Certificate applications (including as required under the *Information Privacy Act 2009* (Qld)) and for use of the Certificate services.
- It has not and will not infringe any third party intellectual property rights in connection with its role in and use of the AusCERT PKI Certificate services.
- It will comply with this CPS and its internal or published policies and procedures.
- It will comply with applicable Australian and local laws and regulations.

- A digital signature created using the private key corresponding to the public key included in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is properly operational at the time the digital signature is created.
- No unauthorized person has ever had access to the Subscriber's private key.
- All representations made by the Subscriber to AusCERT regarding the information contained in the Certificate are accurate and true.
- All information contained in the Certificate is accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber had notice of such information whilst the Subscriber shall act promptly to notify AusCERT and/or Participant Organisation of any material inaccuracies in such information.
- The Certificate is used and will continue to be used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use an AusCERT Certificate only in conjunction with the entity named in the Organisation field of a Certificate (if applicable).
- The Subscriber retains control of its private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The Subscriber is an end-user Subscriber and not a CA, and will not use the private key corresponding to any public key listed in the Certificate for purposes of signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise, unless expressly agreed in writing between Subscriber and AusCERT.
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of AusCERT.
- The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, privacy and personal information, viruses, accessing computer systems etc.
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

Unless otherwise stated in this CPS, Subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally within their Participant Organisation.
- To generate their own private / public key pair to be used in association with the Certificate request submitted to AusCERT.
- To delegate to the Participant Organisation RA the right to generate private / public key pair to be used in association with the Certificate request submitted to AusCERT on their behalf.
- Ensure that the public key submitted to AusCERT corresponds with the private key used.
- Ensure that the public key submitted to AusCERT is the correct one.
- Provide correct and accurate information in its communications with AusCERT.
- Alert AusCERT if at any stage whilst the Certificate is valid, any information originally submitted has changed since it had been submitted to AusCERT.
- Generate a new, secure key pair to be used in association with a Certificate that it requests from AusCERT.
- Read, understand and agree with all terms and conditions in this AusCERT CPS and associated policies published in the AusCERT Repository at cs.auscert.org.au/repository/.
- Refrain from tampering with an AusCERT Certificate.
- Use AusCERT Certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.

- Cease using an AusCERT Certificate if any information in it becomes misleading obsolete or invalid.
- Cease using an AusCERT Certificate if such Certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain from using the Subscriber's private key corresponding to the public key in an AusCERT issued Certificate to issue end-entity Certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in an AusCERT Certificate.
- Request the revocation of a Certificate in case of an occurrence that materially affects the integrity of an AusCERT Certificate.
- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their private keys.

9.6.5. Relying Party Representations and Warranties

A party relying on an AusCERT Certificate accepts that in order to reasonably rely on an AusCERT Certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected Certificate; the Relying Party must have reasonably made the effort to acquire sufficient knowledge on using Certificates and PKI.
- Study the limitations to the usage of AusCERT Certificates.
- Read and agree with the terms of the AusCERT CPS and Relying Party Agreement.
- Verify an AusCERT Certificate by examining the information available through AusCERT's OCSP.
- Trust an AusCERT Certificate only if it is valid and has not been revoked or has expired.
- Rely on an AusCERT Certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

9.6.6. Representations and Warranties of Other Participants

Partners of the AusCERT service shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the AusCERT products and services. Failure to comply with this will result in the termination of the agreement with the Participant Organisation, the removal of permission to use or access the AusCERT Repository and any Certificate or Service provided by AusCERT.

9.7. Limitations of Liability

The exclusive remedy of a party who has paid fees directly to AusCERT in connection with the services described in this CPS for any defect in a product or service for which AusCERT is responsible shall be to have AusCERT attempt through commercially reasonable efforts to arrange for Comodo to attempt to correct or cure any reproducible defect in relation to a Certificate notified to AusCERT by Participant Organisation by issuing corrected instructions, a restriction, or a bypass, or, in the event that Comodo does not correct or cure the material defect in twenty-five (25) business days, to arrange for a pro-rata refund of the amount paid for the defective product. This remedy applies only to the extent AusCERT is able to procure such remedy from Comodo under AusCERT's Sub CA Agreement with Comodo. AusCERT is not obligated to seek correction of a defect or a pro rata refund if the party seeking the refund (a) misused, damaged, or modified the Certificate, (b) did not promptly report the defect to AusCERT, or (c) has breached any provision of this CPS. AusCERT excludes liability to a party who has not paid fees directly to AusCERT in connection with the services described in this CPS.

In no event (except for fraud or willful misconduct) shall AusCERT be liable for:

- Any indirect, incidental or consequential damages;
- Any loss of profits;

- Any loss of data;
- Any other direct, indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of Certificates or digital signatures;
- Any other transactions or services offered within the framework of this CPS;
- Any damage incurred due to fraud or willful misconduct of an Applicant;
- Any liability that arises from the usage of a Certificate that has not been issued or used in conformance with this CPS or the intended use of the ordered Certificate as described on the AusCERT website or elsewhere;
- Any liability that arises from the usage of a Certificate that is not valid;
- Any liability that arises from usage of a Certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CPS;
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses; or
- Any liability that arises from compromise of a Subscriber's private key.

Notwithstanding the foregoing, AusCERT does not limit or exclude liability for death or personal injury.

9.8. Indemnities

9.8.1. Participant Organisation Indemnity to AusCERT

Participant Organisations agree to indemnify and hold AusCERT harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees that AusCERT may incur, that are caused by the use or publication of a Certificate and that arises from:

- Any false or misrepresented data supplied by the Participant Organisation.
- Any failure of the Participant Organisation to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, AusCERT, or any person receiving or relying on the Certificate.
- Failure to protect the Participant Organisation's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Participant Organisation's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to privacy and personal information, intellectual property protection, viruses, accessing computer systems etc.

9.8.2. Subscriber Indemnity to AusCERT

By accepting a Certificate, the Subscriber agrees to indemnify and hold AusCERT, as well as its Participant Organisations and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that AusCERT, and the above mentioned parties may incur, that are caused by the use or publication of a Certificate, and that arises from:

- Any false or misrepresented data supplied by the Subscriber or agent(s).
- Any failure of the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, AusCERT, or any person receiving or relying on the Certificate.
- Failure to protect the Subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's confidential data.

- Breaking any laws applicable in his/her country or territory including those related to privacy and personal information, intellectual property protection, viruses, accessing computer systems etc.

For Certificates issued at the request of a Subscriber's agent, the Subscriber shall indemnify AusCERT.

9.8.3. Subscriber Indemnity to Relying Parties

Without limiting other Subscriber obligations stated in this CPS, Subscribers are liable for any misrepresentations they make in Certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the Certificate.

9.9. Term and Termination

9.9.1. Term

This CPS and any amendments hereto shall become effective seven (7) days after being published to the AusCERT Repository and shall remain effective until terminate in accordance with this Section 9.10.

9.9.2. Termination

This CPS and any amendments hereto shall remain effective until replaced with a newer version.

9.9.3. Effect of Termination and Survival

In case of termination of CA operations for any reason whatsoever, AusCERT will provide timely notice. Before terminating its own CA activities, AusCERT will take the following steps, where possible:

- Providing Subscribers of valid Certificates with 90 days' notice of its intention to cease acting as a CA.
- Revoking all Certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking Subscriber's consent.
- Giving timely notice of revocation to each affected Subscriber.
- Making reasonable arrangements to preserve its records according to this CPS.
- Reserving its right to provide succession arrangements for the re-issuance of Certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as AusCERT's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

9.10. Individual notices and Communications with Participants

AusCERT accepts notices related to this CPS by means of digitally-signed messages or in paper form. Upon receipt of a valid digitally-signed acknowledgment of receipt from AusCERT, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within 10 days, or else the communication shall not be deemed effective and written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

AusCERT Certification Authority
AusCERT
The University of Queensland
QLD 4072
Australia

9.11. Amendments

The AusCERT Certificate Policy Authority is responsible for determining the suitability of Certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

9.11.1. Procedure for Amendment

Amendments to this CPS may be made from time to time by AusCERT. Amendments shall either be in the form of an amended form of the CPS or made available as a supplemental document on the AusCERT Repository. Updates supersede any designated or conflicting provisions of the referenced version of the CPS and shall be indicated through appropriate revision numbers and publication dates. Revisions that are not deemed significant by AusCERT (those amendments or additions that have minimal or no impact on Subscribers or Relying Parties), shall be made without notice and without changing the version number of this CPS.

Controls are in place to reasonably ensure that the AusCERT CPS is not amended and published without the prior authorization of the AusCERT Certificate Policy Authority.

9.11.2. Notification Mechanism and Period

Updated editions of the CPS will be published at the AusCERT Repository (available at cs.auscert.org.au/repository/), with seven (7) days' notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

9.11.3. Circumstances Under Which OID Must be Changed

If AusCERT decides that a change in AusCERT's Certificate Policy or Certificate Practices warrants a change in the currently specified OID for a particular Certificate type, then the revised CPS or amendment thereto will contain a revised OID for that type of Certificate.

9.12. Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify AusCERT of the dispute with a view to seek dispute resolution.

9.13. Governing Law

This CPS is governed by, and construed in accordance with the laws of Queensland, Australia. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of AusCERT Certificates or other products and services. Queensland law applies in all AusCERT commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to AusCERT products and services where AusCERT acts as a provider, supplier, beneficiary receiver or otherwise.

9.14. Jurisdiction

Each party, including AusCERT partners, Subscribers and Relying Parties, irrevocably agrees that the courts of Queensland, Australia have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of AusCERT PKI services.

9.15. Miscellaneous Provisions

9.15.1. Interpretation

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service.

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.15.2. Assignment

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not affect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.15.3. Severability

If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to affect the original intention of the parties.

Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.15.4. Enforcement and waiver

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision. Agreements between AusCERT and the parties detailed in this CPS may contain additional provisions governing enforcement and shall be enforced according to the terms and conditions set forth within each respective agreement.

AusCERT may seek indemnification and attorneys' fees from any party that violates their individual agreements with AusCERT or whose conduct is in violation of this CPS. Except where an express time frame is set forth in this CPS any delay or omission by any party shall not impair or be construed as a waiver of such right, remedy or power.

9.15.5. Force Majeure

AusCERT shall not be liable for any breach of its obligations, representations, warranties, or for its failure to perform where such failure or breach is as a result of a Force Majeure Event., including, but not limited to, fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalization, government sanction, blockage, embargo, labor dispute, strike, lockout or interruption or failure of electricity or telephone service or any other system operated by any other party over which AusCERT has no control, or other similar causes beyond AusCERT's reasonable control where AusCERT is without fault or negligence.

9.16. Other Provisions

9.16.1. Refusal to Issue a Certificate

AusCERT and Comodo reserve the right to refuse to issue a certificate to any party as they see fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. AusCERT and Comodo reserve the right not to disclose reasons for such a refusal.

9.16.2. Legality of Information

Participant Organisations and Subscribers shall each be responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

9.16.3. Subscriber Liability to Relying Parties

Without limiting other Participant Organisation or Subscriber obligations stated in this CPS, Participant Organisations and Subscribers are liable for any misrepresentations they make in certificates to third

parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

9.16.4. Duty to Monitor Agents

The Subscriber shall control and be responsible for the data that is supplied to AusCERT for a Certificate, whether by the Subscriber or an agent of the Subscriber.

9.16.5. Conditions of usage of the AusCERT Repository and Web site

Parties (including Subscribers and Relying Parties) accessing the AusCERT Repository and official web site(s) agree with the provisions of this CPS and any other conditions of usage that AusCERT may make available.

Parties demonstrate acceptance of the conditions of usage of the CPS by using an AusCERT issued certificate.

Failure to comply with the conditions of usage of the AusCERT Repository and web site may result in terminating the relationship between AusCERT and the party.

9.16.6. Accuracy of Information

AusCERT and the Participant Organisations, recognising their trusted position, make all reasonable efforts to ensure that parties accessing the AusCERT Repository receive accurate, updated and correct information. AusCERT and the Participant Organisations however, cannot accept any liability beyond the limits set in this CPS.

9.16.7. Non-Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this CPS, AusCERT shall not be responsible for non-verified Subscriber information submitted to AusCERT or otherwise submitted with the intention to be included in a certificate.

APPENDIX A

AusCERT CA KEYS

CA Number	Description	Usage	Lifetime	Size
1	AusCERT Server CA	<p>Intermediate Certificate to issue the following Certificates:</p> <ul style="list-style-type: none"> Single Server OV SSL Certificates Single Server OV Wildcard SSL Certificates MDC SSL Certificates (up to 100 domains) 	<i>Saturday, May 30, 2020 6:48:38 AM</i>	2048
2	AusCERT SGC Server CA	<ul style="list-style-type: none"> SGC SSL Certificates SGC Wildcard Certificates 	<i>Saturday, May 30, 2020 6:48:38 AM</i>	2048
3	AusCERT Code Signing CA	<p>Intermediate Certificate to issue the following Certificates:</p> <ul style="list-style-type: none"> Code Signing Certificates 	<i>Saturday, May 30, 2020 6:48:38 AM</i>	2048
4	AusCERT Client CA	<p>Intermediate Certificate to issue the following Certificates:</p> <ul style="list-style-type: none"> Email and Client Authentication Certificates (S/MIME) 	<i>Saturday, May 30, 2020 6:48:38 AM</i>	2048

APPENDIX B

CERTIFICATE TYPES

AusCERT Certificate offerings may include the following types of Certificates:

- **Organisation Validated Certificates**

Organisation Validated (OV) Certificates are issued to both individuals and Organisations whose identities have first been verified according to the validation procedures described in Section 4. It includes Single Server OV SSL Certificates and Single Server OV Wildcard SSL Certificates

- **SGC SSL Certificates**

SGC SSL Certificates are professional level Server Gated Cryptography (SGC) enabled Certificates designed to upgrade the encryption capabilities of older browsers from 40-bit encryption into full 128/256 bit encryption. SGC are validated as OV Certificates and include SGC SSL Certificates and SGC Wildcard Certificates.

- **Wildcard Certificates**

Wildcard Certificates are used to secure multiple sub-domains with a single Certificate. Wildcard Certificates may be OV or SGC Certificates.

- **MDCs**

Multi Domain Certificates (MDCs) are OV SSL Server Certificates issued by AusCERT as a means of validation of domain control for the domains jointly hosted on a single server and named within the MDC. MDC may be used for up to 100 domains within the validated Organisation.

- **UCCs**

Unified Communications Certificates are used to cover multiple unique domains within a single Certificate. UCCs are validated as OV SSL Server Certificates.

- **Personal Validated Certificates (Email and Client Certificates (S/MIME))**

Personal Validated Email and Client Certificates are used to encrypt email and digitally sign documents (Standard and High).

- **Code Signing**

Code Signing Certificates enable developers to digitally sign their software before distribution over the Internet.

APPENDIX C

PKI HEIRARCHY

1. 3 year SSL and Wildcard SSL certificates / Multi-Domain certificates / Unified Communication Certificates

Visible on IE compatible browsers as follows:

UTN-USERFIRST-Hardware (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2a fe 65 0a fd, expiry = 09 July 2019 19:19:22*)

↳ AusCERT Server CA (*serial number = 61 f8 58 a7 b9 81 57 93 34 9d 7e 19 bb 8a 10 99, expiry = 30 May 2020 6:48:38 AM*)

↳ End Entity SSL (*serial number = x, expiry = 1-3 years from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows:

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

↳ UTN-USERFirst-Hardware (*serial number = 48 4b ac f1 aa c7 d7 13 43 d1 a2 74 35 49 97 25, expiry = 30 May 2020 11:48:38*)

↳ AusCERT Server CA (*serial number = 61 f8 58 a7 b9 81 57 93 34 9d 7e 19 bb 8a 10 99, expiry = 30 May 2020 6:48:38 AM*)

↳ End Entity SSL (*serial number = x, expiry = 1-3 years from issuance*)

2. SGC / SGC Wildcard Certificates

Visible on IE compatible browsers as follows:

UTN - DATACorp SGC (*serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019 20:06:40*)

↳ AusCERT SGC Server CA (*serial number = 0f 45 f4 01 eb 20 a8 19 98 2d a8 b0 45 fa 34 32, expiry = 30 May 2020 6:48:38 AM*)

↳ End Entity SSL (*serial number = x, expiry = 1- 3 years from issuance*)

Cross signed and therefore visible on Netscape compatible browsers as follows:

AddTrust External CA Root (*serial number = 01, expiry = 30/05/2020 10:48:38*)

↳ UTN - DATACorp SGC (*serial number = 53 7b 76 56 4f 29 7f 14 dc 69 43 e9 22 ad 2c 79, expiry = 30 May 2020 11:48:38*)

↳ AusCERT SGC Server CA (*serial number = 0f 45 f4 01 eb 20 a8 19 98 2d a8 b0 45 fa 34 32, expiry = 30 May 2020 6:48:38 AM*)

↳ End Entity SSL (*serial number = x, expiry = 1 month or up to 10 year(s) from issuance*)

3. Code Signing Certificates

UTN-USERFirst-Object (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2d e0 b3 5f 1b, expiry = 09 July 2019 19:40:36*)

↳ AusCERT Code Signing CA (*serial number = 23 7e 74 5c 59 77 01 e1 69 79 1a b8 fc d2 0d ca, expiry = Saturday, May 30, 2020 6:48:38 AM*)

↳ End Entity Code Signing (*serial number = x, expiry = 1 month or up to 5 year(s) from issuance*)

4. Client Certificates

UTN-USERSFirst-Client Authentication and Email (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 c9 89*,
expiry = 09 July 2019 18:36:58)

↳ AusCERT Client CA (*serial number = 4d e7 ad 3c e3 c0 f3 2c 70 4d f7 71 a1 29 92 a4*,
expiry = Saturday, May 30, 2020 6:48:38 AM)

↳ End Entity Client and Email Certificate (*serial number = x*, *expiry = 1 month or up to 3*
year(s) from issuance)

APPENDIX D

CERTIFICATE POLICIES

AusCERT OV Certificates: TLS Certificates, Wildcard Certificates, MDCs, SGC and UC
Terms and Conditions of use: <http://cs.auscert.org.au/repository>

Version	V3	
Serial number	<Serial number>	
Signature Algorithm	sha1RSA	
Issuer (non-SGC)	CN	AusCERT Server CA
	OU	Certificate Services
	OU	
	O	AusCERT
	C	AU
	CN	AusCERT SGC Server CA
Issuer (SGC)	OU	Certificate Services
	OU	
	O	AusCERT
Validity	C	AU
	1 / 2 / 3 year(s)	
	CN	<Domain Name> (required)
	O	<Participant Organisation Name> (required)
	OU	<Participant Organisation Unit Name> (optional)
	L	<Locality of Participant Organisation> (per Organisation) (optional)
Subject	streetAddress1	<Street Address> (optional)
	streetAddress2	<Street Address> (optional)
	ST	<State of Participant Organisation> (optional) (per Organisation)
	PostalCode	<Zip or Postal Code> (optional)
	postOfficeBox	<PoBox> (optional)
	unstructuredName	Contains a domain name (optional)
	C	<Country of Participant Organisation> (required)

Subject Alternative Name (MDCs and UCCs only)	<i>DNS Name=<Domain Name 1> DNS Name=<Domain Name 2> DNS Name=<Domain Name 3>up to DNS Name=<Domain Name 100></i>
Public Key	<2048 bit Public Key>
Authority Key Identifier (Non-Critical)	KeyID = <Unique ID of the issuer's public key>
Key Usage (Critical)	Digital Signature, Key Encipherment(A0)
Subject Key Identifier (Non-Critical)	<Unique ID of the subject's public key>
Certificate Policies (Non-Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.23485.5.1.1.0
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cs.auscert.org.au/AusCERTServerCA.crl URI:http://crl.cs.auscert.org.au/AusCERTServerCA.crl
CRL Distribution Points (SGC)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cs.auscert.org.au/AusCERTSGCServerCA.crl URI:http://crl.cs.auscert.org.au/AusCERTSGCServerCA.crl
Authority Information Access (Non-Critical)	[1] <i>AccessMetohd=CA Issuers</i> <i>Location=</i> http://crt.cs.auscert.org.au/AusCERTServerCA.crt [2] <i>AccessMethod=OCSP</i> <i>Location=</i> http://ocsp.cs.auscert.org.au
Authority Information Access (SGC) (Non-Critical)	[1] <i>AccessMetohd=CA Issuers</i> <i>Location=</i> http://crt.cs.auscert.org.au/AusCERTSGCServerCA.crt [2] <i>AccessMethod=OCSP</i> <i>Location=</i> http://ocsp.cs.auscert.org.au
Key Usage	Digital Signature, Key Encipherment(A0)
Extended Key Usage (non-SGC) (Non-Critical)	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
Extended Key Usage (SGC) (Non-Critical)	TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)

Basic Constraints	Netscape Server Gated Crypto (2.16.840.1.113730.4.1) Microsoft Server Gated Crypto (1.3.6.1.4.1.311.10.3.3) Subject Type=End Entity Path Length Constraint=0
Thumbprint algorithm	Sha1
Thumbprint	<Thumbprint>

AusCERT Personal Certificates: Standard, High (ID validated)		
Terms and Conditions of use: http://cs.auscert.org.au/repository		
Version	V3	
Serial number	<Serial number>	
Signature Algorithm	sha1RSA	
Issuer	CN	AusCERT Client CA
	OU	
	OU	Certificate Services
	O	AusCERT
	C	AU
Validity	1 / 2 / 3 year(s)	
Subject	CN	<Applicant's Name> (required)
	O	<Participant Organisation Name> (required)
	OU	<Participant Organisation Unit Name> (optional)
	L	<Locality of Participant Organisation> (per Organisation) (optional)
	streetAddress1	<Street Address> (optional)
	streetAddress2	<Street Address> (optional)
	ST	<State of Participant Organisation> (optional) (per Organisation)
	PostalCode	<Zip or Postal Code> (optional)
	postOfficeBox	<PoBox> (optional)
	unstructuredName	Contains additional email address (optional)
	C	<Country of Participant Organisation> (required)

Public key	2048 bit public key
Authority Key Identifier (Non-Critical)	KeyID = <Unique ID of the issuer's public key>
Key Usage (Critical)	Digital Signature, Key Encipherment(A0)
Subject Key Identifier (Non-Critical)	<Unique ID of the subject's public key>
Extended Key Usage (Non-Critical)	id-kp-emailProtection, id-kp-clientAuth(1.3.6.1.5.5.7.3.2), Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
Basic Constraint (Critical)	Subject Type = End entity Path Length Constraint= 0
Certificate Policies (Non-Critical)	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.23485.5.1.1.0.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.23485.5.1.1.0.3
CRL Distribution Policies (Non-Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cs.auscert.org.au/AusCERTClientCA.crl URI:http://crl.cs.auscert.org.au/AusCERTClientCA.crl
Authority Information Access	[1] <i>AccessMethod=CA Issuers</i> <i>Location</i> =http://crl.cs.auscert.org.au/AusCERTClientCA.crt
(Non-Critical)	[2] <i>AccessMethod=OCSP</i> <i>Location</i> = http://ocsp.cs.auscert.org.au
Subject Alternative Name (Non-Critical)	rfc822Name (min 1, max 10 email addresses) otherName.userPrincipalName (min 0, max 1 UPN) ¹
Thumbprint algorithm	Sha1
Thumbprint	<Thumbprint>

¹ See <http://support.microsoft.com/kb/281245>. User Principle Name (UPN). The UPN OtherName OID is : "1.3.6.1.4.1.311.20.2.3". The UPN OtherName value: Must be ASN1-encoded UTF8 string for example user@org.edu.au

AusCERT Code Signing Certificates**Terms and Conditions of use:** <http://cs.auscert.org.au/repository>

Version	V3	
Serial number	<Serial number>	
Signature Algorithm	sha1RSA	
Issuer	CN	AusCERT Code Signing CA
	OU	
	OU	Certificate Services
Validity	O	AusCERT
	C	AU
	1 / 2 / 3 year(s)	
Subject	CN	<Applicant's Name> (required)
	O	<Participant Organisation Name> (required)
	OU	<Participant Organisation Unit Name> (optional)
	L	<Locality of Participant Organisation> (per Organisation) (required)
	streetAddress1	<Street Address> (required)
	streetAddress2	<Street Address> (optional)
	ST	<State of Participant Organisation> (required) (per Organisation)
	PostalCode	<Zip or Postal Code> (required)
	postOfficeBox	<PoBox> (optional)
	unstructuredName	Contains additional email address (optional)
	C	<Country of Participant Organisation> (required)
Public key	2048 bit public key	
Authority Key Identifier (Non-Critical)	KeyID = <Unique ID of the issuer's public key>	
Key Usage (Critical)	Digital Signature	
Subject Key Identifier (Non-Critical)	<Unique ID of the subject's public key>	
Extended Key Usage (Non-Critical)	id-kp-codeSigning	

Basic Constraint (Critical)	Subject Type = End entity Path Length Constraint= 0
Certificate Policies (Non-Critical)	[1] Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.23485.5.1.1.0
CRL Distribution Policies (Non- Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cs.auscert.org.au/AusCERTCodeSigningCA.crl URI:http://crl.cs.auscert.org.au/AusCERTCodeSigningCA.crl [1] AccessMethod=CA Issuers Location=http://crl.cs.auscert.org.au/AusCERTCodeSigningCA.crl
Authority Information Access (Non-Critical)	[2] AccessMethod=OCSP Location= http://ocsp.cs.auscert.org.au
Thumbprint algorithm	Sha1
Thumbprint	<Thumbprint>