Australian Government
Australian Taxation Office

X.509 Certification Practice Statement

ATO PKI

Version control

Version	Date	Description of change
0.1	8 August 2018	Migration from AUSkey Policy
1.0	27 March 2019	Final Version post legal review
1.1	9 August 2021	Review pre-IP3 release
1.2	30 October 2024	Review & Update with new CPs

We acknowledge the Traditional Owners and Custodians of Country throughout Australia and their continuing connection to land, waters and community.
We pay our respects to them, their cultures, and Elders past and present.

Contents

1 Introduction

This document is the Certification Practice Statement (CPS). A CPS is a statement of the practices that a Certification Authority (CA) employs in issuing, managing, revoking, re-keying, and renewing digital Certificates.

The headings in this CPS follow the framework set out in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

This CPS provides Australian Taxation Office (ATO) Public Key Infrastructure (PKI) Community of Interest (COI) members with a description of the practices followed in order to indicate the level of trust that may be placed in certificates issued by the ATO Root CA and it's subordinate CAs. However, some security practices are too sensitive to be described in this CPS and are described in classified documents instead.

Other parties who may be expected to read this CPS include:

- the ATO PKI System Owner or their delegates;
- regulators and accreditors, such as Australian Signals Directorate (ASD) and the Digital Transformation Agency (DTA);
- auditors; and
- ATO PKI Operations personnel (PKI Operators).

This CPS is complemented by a number of Certificate Policies (CPs) which serve a policy function – each CP promulgates the rules applying to a particular type of Certificate.

This introductory section identifies and introduces the set of provisions, and indicates the types of entities and applications this CPS applies to.

1.1 Overview

The purpose of this CPS is to provide a common framework under which the ATO PKI, CA, and Registration Authority (RA) services are provided. As such it sets out a number of policy and operational matters related to the services, including the practices that the ATO employs in issuing, revoking, and managing certificates.

This CPS describes the practices followed by the ATO CA in relation to Certificates issued from the ATO PKI to reliant applications. Reliant applications include myID, the Relationship Authorisation Manager (RAM), and the ATO Identity Provider (IdP). myID is a program established by the ATO intended to improve the user experience through increased convenience and flexibility when interacting digitally with Government. The RAM is intended to fulfill this same purpose, but in the context of organisations interactions with Government. The ATO IdP provides secure access to ATO Online Services for individuals. The ATO PKI has been established to deliver CA and RA services for these Programs.

The Community of Interest (COI) for ATO PKI Certificates is restricted to:

- Individuals (both Australian and Foreign citizens) that are required to interact with services that accept myID, RAM, and/or ATO IdP credentials for authentication, and
- Organisations (both Australian and Foreign) that are required to interact with services that accept myID, RAM, and/or ATO IdP credentials for authentication.

myID provides a credential solution leveraging the Fast Identity Online (FIDO) framework combined with PKI. The myID System will provide a replacement solution for the AUSid and Standard Business Reporting (SBR) AUSkey programs. Certificates issued to ATO PKI-reliant systems are only designed for users to authenticate themselves to, and carry out electronic transactions with, ATO PKI COI member Relying Parties – see sections 1.1.1 and 1.3.4.

The ATO PKI conducts its role in accordance with the Approved Documents. The Approved Documents comprise:

- The following public documents:
- This CPS;
  - The X.509 Certificate Policy for the ATO **myID User**;
  - The X.509 Certificate Policy for the ATO **Business Machine**;
  - The X.509 Certificate Policy for the ATO **Online User**;
  - The X.509 Certificate Policy for the ATO **Online Device**;
  - The X.509 Certificate Policy for the ATO **Server Identity**;
  - The ATO PKI myID **Terms of Use - User**;
  - The ATO PKI myID **Terms of Use – Machine**;
  - The ATO PKI myID **Privacy Policy**.
- The following classified documents:
  - The myID Information Security Policy (ISP);
  - The myID System Security Plan (SSP);
  - The myID Security Risk Management Plan (SRMP);
  - The myID Cryptographic Key Management Plan (CKMP);
  - The myID Disaster Recovery and Business Continuity Plan (DRBCP);
  - The myID Incident Response Plan (IRP);
  - The myID Personnel Security Plan (PSP);
  - The myID Vulnerability Management Plan (VMP);
  - The myID Certificate Authority Operations Manual (CA OpsMan);
  - The myID Standard Operating Procedures (SOPs); and
  - The Gatekeeper Memorandum of Agreement (MOA).

Whilst the classified documents are named in this CPS, the contents are not disclosed publicly for security reasons.

The ATO operates a PKI that complies with this CPS and the PKI is capable of supporting multiple CAs to provide difference certificate types.

The following Certification Authorities are covered under this CPS:

OID	Certification Authority
1.2.36.1.9001.1.1.1	ATO Root Certification Authority (ATO RCA)
1.2.36.1.9001.1.1.1.1	ATO Subordinate Certificate Authority (ATO CA)

1.1.1 Community of Interest

The ATO PKI COI consists of Relying Parties (who accept credentials supplied by ATO PKI-relaint applications) and Individuals and Organisations (who holdcredentials supplied by ATO PKI-reliant applications). For the purposes of the ATO PKI COI:

- the **Relying Parties** are Entities that support myID, RAM, and/or ATO IdP credentials for authentication and authorisation, where "Entity" can mean:
  - A Department of State, or a Department of the Parliament, of the Commonwealth, a State or a Territory;
  - A body corporate or an unincorporated body established or constituted for a public purpose by Commonwealth, State or Territory legislation, or an instrument made under that legislation (including a local authority);
  - A body established by the Governor General, a State Governor, or by a Minister of State of the Commonwealth, a State or a Territory;
  - An incorporated company over which the Commonwealth, a State or a Territory has a controlling interest; or
  - A privately incorporated or unincorporated company, business, or organisation.
- the **Individuals** are entities:
  - Willing and able to present valid and verifiable identity information to the ATO for confirmation of proof of identity;
  - Willing and able to utilise the myID, RAM, and/or ATO IdP service(s); and
  - Seeking to authenticate to myID, RAM, and/or ATO IdP enabled services.
- the **Organisations** are entities:
  - Willing and able to present valid and verifiable identity information to the ATO for confirmation of proof of identity;
  - Willing and able to utilise the myID, RAM, and/or ATO IdP service(s); and
  - Seeking to authenticate to myID, RAM, and/or ATO IdP enabled services.
- Participation in the ATO PKI COI:
  - For Relying Parties – is restricted to those Agencies that engage electronically for authentication to services; and

- For Citizens of the Commonwealth of Australia (CoA) and Foreign National Individuals and Organisations - is not restricted for participation at Identity Proofing (IP) level 0 and 1. Attainment of higher levels of assurance within the myID service is subject to satisfying the IP requirements defined under the Trusted Digital Identity (ID) Framework (TDIF).

1.2 Document Name and Identification

This document is known as the *Certification Practice Statement*. It does not require an object identifier (OID). (The format for OIDs for the associated Certificate Polices is set out in Appendix A). This CPS can be accessed online at http://pki.ato.gov.au/policy/ca.html.

1.3 PKI Participants

1.3.1 Certification Authorities

1.3.1.1 ATO Root Certification Authority (ATO RCA)

The ATO RCA is the self-signed trust point of the ATO PKI Certificate hierarchy. The ATO RCA only signs and renews the ATO CA's Certificate, and renews its own Key and Certificate. The ATO RCA's system is therefore kept offline most of the time and is secured as described in sections 5 and 6.

1.3.1.2 ATO Certification Authority (ATO CA)

The ATO CA is the single operational Certification Authority in the ATO PKI Certificate hierarchy. The ATO CA is responsible for generating CRLs and Certificates for reliant applications including myID, RAM, and ATO IdP.

Note: although the ATO CA generates Certificates for reliant systems, the Subscriber's Private Keys are generated by the end user - the End Entity unless otherwise stated in the relevant CP. The ATO CA's own Certificate is signed by the ATO RCA.

1.3.2 Registration Authorities

The *Registration Authority (RA)*, or RAs, that perform the registration function under this CPS are ATO RAs or ATO approved "Third Party" RAs (Authorised RAs). An RA is formally bound to perform the registration functions in accordance with the applicable CP and other relevant documentation via an appropriate agreement with the ATO.

- Gatekeeper accredited CAs must only use Gatekeeper accredited RAs; and
- Non-Gatekeeper accredited CAs may use ATO RAs, Authorised RAs, or Gatekeeper accredited RAs as approved by the ATO PKI System Owner.

All ATO-internal RA systems are a combination of ATO developed software components working in conjunction with external services to accept relevant requests, capture EOI information, verify EOI by calling on verification subsystems, and is integrated with ATO services. Core RA services are provided

by the myID Identity Services, ATO IdP Identity Services, and the MAS-RA. There is no direct end-user interface with any ATO RA. Instead, users interact through ATO applications, which connect to applications according to defined APIs. This promotes usability, consistency, and disguises the complexities of the underlying systems whilst preserving the strong security of Public Key technology.

1.3.3 Subscribers

A subscriber is defined to be, as the context allows:

- The entity (e.g. a myID user or device custodian) whose Distinguished Name or other uniquely identifying information appears as the "Subject Distinguished Name" on the relevant Certificate, and/or,
- The person or legal entity that applied for that Certificate, and/or entered into the Subscriber Agreement in respect of that Certificate.

Certificates issued by the ATO RCA or ATO CA to the operators of core components will not be used as a validation mechanism for that individual. All such certificates will only be valid for use within the PKI core components.

Individual CPs provide context for the definition of Subscriber relevant to that CP.

1.3.4 Relying Parties

In general, a *Relying Party* uses an ATO certificate to:

- Verify the identity of an entity;
- Verify the integrity of a communication with an entity;
- Establish confidential communications with an entity; and
- Ensure the non-repudiation of a communication with an entity.

In order to provide uninhibited access to revocation information and subsequently invoke trust in its own services, the ATO refrains from implementing an agreement with Relying Parties with regard to controlling the validity of certificate services with the purpose of binding Relying Parties to their obligations.

Use of the ATO PKI by Relying Parties is governed by the conditions set out in the ATO PKI policy framework consisting of the *Approved Documents*.

Relying Parties are hereby notified that the conditions prevailing in the CPS, and relevant CP, are binding upon them when they consult the ATO PKI for the purpose of establishing trust and validation of ATO PKI certificates.

A Relying Party is responsible for deciding whether, and how, to establish:

- The validity of the entity's certificate using certificate status information;
- Any authority, or privilege, of the entity to act on behalf of the ATO; and
- Any authority, access, or privilege the entity has to the Relying Party's assets or systems.

A Relying Party agrees to the conditions of the relevant CP and must:

- Verify the validity of a digital certificate (i.e. verify that the digital certificate is current and has not been revoked or suspended, in the manner specified in the CP under which the digital certificate was issued);
- Verify that the digital certificate is being used within the limits specified in the CP under which the digital certificate was issued; and
- Promptly notify the ATO PKI in the event that it suspects that there has been compromise of the Subscriber's Private Keys.

Other than the chain of trust aspects there are no Relying Parties for the CA certificates issued under this CPS. This chain of trust is created by the ATO RCA signing the ATO CA certificate that signs the certificate issued to the end-entity and the issuance of *Certificate Revocation Lists (CRLs)*.

1.3.5 Other Participants

Other participants include:

- The ATO PKI System Owner – which owns the overarching policy under which this CPS operates, and:
  - Reviews and approve this CPS and relevant CPs;
  - Ensures that the infrastructure remains compliant at all times within the terms of its accreditation;
  - Presides over the PKI audit process;
  - Defines rules, and approves agreements, for interoperation with other PKIs;
  - Approves mechanisms and controls for the management of the PKI;
  - Approves operational standards and guidelines to be followed;
  - Provides strategic direction for *Public Key Technology (PKT)* addressing ATO, National, and International issues;
  - Monitors the governance and performance of the ATO PKI; and
  - Authorises establishing the PKT infrastructure to support PKI within the ATO.
- Accreditation agencies – to provide independent assurance that the facilities, practices, and procedures used to issue ATO certificates comply with the relevant accreditation frameworks (policy, security, and legal);

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued under this CPS, in conjunction with their associated *Private Keys*, allow the ATO RCA to:

- Self-sign the ATO RCA certificate;
- Digitally sign a CA certificate; and
- Sign the operational certificates required by the PKI, including OCSP responder(s).

Certificates issued under this CPS, in conjunction with their associated private keys, allow the ATO CA to:

- Digitally sign end-entity certificates;
- Digitally sign a certificate for any CA subservient to the ATO CA; and
- Sign the operational certificates required by the PKI, including OCSP responder(s).

All other core component certificates will only be valid for use within the PKI and used for the authentication and confidentiality (as appropriate) of core component activities.

For all other appropriate certificate uses, see the relevant CP.

1.4.2 Prohibited Certificate Uses

The prohibited uses for certificates issued under this CPS are:

- For the ATO RCA, to sign certificates issued to end-entity Subscribers;
- To sign the certificate of a non ATO System Owner approved CA;
- To validate the identity of a *PKI Operator*; and
- To establish a Subordinate CA to conduct any transaction, or communication, which is any or all of the following:
  - Unrelated to ATO business;
  - Illegal;
  - Unauthorised;
  - Unethical, or
  - Contrary to ATO Policy.

Engaging in a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the PKI Operators and the ATO disclaims any and all liabilities in such circumstances.

For all other prohibited certificate uses, see the relevant CP.

1.5 Policy Administration

This section defines the administrative details for all aspects of this CPS and any applicable CPs.

1.5.1 Organization Administering the Document

The ATO, through the PKI System Owner, is the endorsing organisation for this CPS and applicable CPs, and any amendments. Additional organisations, through agreement with the PKI System Owner, may also endorse this CPS as satisfying their requirements for a specific CP. The ATO will maintain a list of organisations and certificate types for which such agreement exists.

1.5.2 Contact Person

The contact details for the PKI System Owner are as follows:

PKI System Owner

Australian Taxation Office

PO Box 9977

Civic Square, ACT, 2608

1.5.3 Person Determining CPS Suitability for the Policy

The PKI System Owner is also responsible for determining if the CPS is suitable for a CP.

1.5.4 CPS Approval Procedures

This CPS is approved by the PKI System Owner and the Gatekeeper Competent Authority.

Before accepting changes to this document:

- The proposed changes are to be integrated into a draft document and submitted to the PKI System Owner;
- The proposed changes are reviewed by the PKI System Owner (or their delegate);
- Once the proposed changes are deemed acceptable, the PKI System Owner will endorse the changes and forward the endorsed changes to external parties who perform any PKI accreditation with the ATO; and
- Upon acceptance by all parties, the PKI System Owner will approve for publication, and implementation, the proposed changes.

1.6 Definitions and Acronyms

1.6.1 Definitions

Note that the defined terms in this CPS appear in italics the first time they are used and otherwise are not identified in this manner when appearing later throughout the CPS. Defined terms may be upper or lower case.

Term	Definition
Accreditation Agencies	Those agencies that provide independent assurance that the facilities, practices and procedures used to issue ATO certificates comply with the relevant accreditation frameworks (policy, security and legal). Principally these will consist of DTA, ASD and the ATO ITSA.
Active Directory	Microsoft product used in network and identity management. It uses the Lightweight Directory Access Protocol and typically stores information about all resources on the network. It also provides authentication services and can store PKI certificates.
Affiliated	An entity that is associated with the ATO.
Application	A computer application or relevant component of one (including any object, module, function, procedure, script, macro or piece of code)
Approved Documents	The Approved Documents are those approved by the ATO and include those approved by the Gatekeeper Competent Authority E.g. CPS, CPs, ICTSP, SSP, KMP, DRBCP, IRP and CA Operations Manual.
Authorised RA	Has the meaning given to it in paragraph 1.3.2 of this CPS.
Business Day	Any day other than a Saturday, Sunday or public holiday (including public service holidays) for the whole of the Australian Capital Territory. Traditionally such days are from 0800 to 1600.
Certificate	An electronic document signed by the Certification Authority which: • Identifies a Subscriber by way of a Distinguished Name • Binds the Subscriber to a Key Pair by specifying the Public Key of that Key Pair • Contains the information required by the Certificate Profile.
Certificate Assurance Level	See Level of Assurance.

Term	Definition
Certificate Information	Information needed to generate a digital certificate as required by the Certificate Profile.
Certificate Policy	Means the definition adopted by RFC3647, which defines a Certificate Policy as "A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements".
Certificate Profile	A certificate profile provides details about the format and contents of a digital certificate, including, for a natural person, their Distinguished Name.
Certificate Repository	The Certificate Repository provides a scalable mechanism to store and distribute certificates, cross-certificates and CRLs to end users of the PKI.
Certificate Revocation List	The published directory which lists revoked digital Certificates. The CRL may form part of the Directory or may be published separately.
Certificate Authority	A Certificate Authority (or Certification Authority) is an entity which issues digital certificates for use by other parties.
Certificate Store	Storage location for certificates on a computer or device.
Certification Practice Statement	A statement of the practices that a Certification Authority employs in managing the digital Certificates it issues (this includes the practices that a Registration Authority employs in conducting registration activities on behalf of that Certification Authority). These statements will describe the PKI certification framework, mechanisms supporting the application, insurance, acceptance, usage, suspension/revocation and expiration of digital Certificates signed by the CA, and the CA's legal obligations, limitations and miscellaneous provisions.
Code Signing	Process of digitally signing software code, i.e. scripts or executables, to attest to the authenticity and integrity of the code, and to the identity of the publisher.

Term	Definition
Commonwealth	Means the Commonwealth of Australia
Commonwealth Agency	An agency established by the Commonwealth or in which the Commonwealth has a controlling interest.
Core Components	Core components include the following: • ATO Root Certificate Authority (RCA) – self-signed root trust point of the PKI; • ATO Root Certificate Authority Operators (ATO RCAO); • ATO Certificate Authority (ATO CA); • ATO Certificate Authority Operators (ATO CAO); and • Registration Authority (RA).
Cross-certification	The establishment of a trust relationship between two PKIs, where one CA signs another PKI's CA certificate. This creates a chain of trust allowing the subscribers of the cross-certifying CA to trust those of the cross-certified CA. If done two-ways (PKIs signing each other's CAs' certificates), mutual trust can be established.
Cross-certification ceremony	The event where a cross-certification agreement is executed, i.e. one CA creates a cross-certification request to another CA. The cross-signing CA creates and returns the cross-certificate, signed with its own private key. The "ceremony" is a formal event, and is witnessed by representatives of both CAs. Details of the event are recorded and signed by the witnesses to provide an audit record.
Custodian	A person who has custody of something, a keeper or guardian; in the context of PKI, usually a Key Custodian. See also Resource Custodian.
Device	Device means any computer hardware or other electronic device.
Digital Signature	An electronic signature created using a Private Signing Key.

Term	Definition
Distinguished Name (DN)	An unique identifier assigned to, as relevant: • The Subscriber identified by; and • The issuer of a Certificate, having the structure required by the Certificate Profile
Evaluated Product List (EPL)	The Evaluated Product List is produced to assist in the selection of products that will provide an appropriate level of information security. The list, maintained by ACSC, is published at https://www.cyber.gov.au/acsc/view-all-content/epl-products. The EPL lists products that: • Have completed Common Criteria (CC) or ITSEC certification, • Are in evaluation within the AISEP, or • Have completed some other recognised ASD evaluation methodology.
Evaluation Assurance Level (EAL)	The Evaluation Assurance Level (EAL1 through EAL7) of a computer product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented.
Evidence Of Identity	Evidence (e.g. in the form of documents) issued to substantiate the identity of the presenting party, usually produced at the time of Registration (i.e. when authentication credentials are issued).
Exercised	To discharge, or perform, a function. Or, an act of employing or putting into play.
Force Majeure	A Force Majeure event means any occurrence or omission that is beyond the reasonable control of a party that prevents that party from, or delays that party in, performing any of its obligations under this CPS, a CP or a Subscriber Agreement, including, where relevant, due to forces of nature, war, riot, civil commotion, failure of a public utility, or industrial action (other than industrial action specifically directed at a party).

Term	Definition
Gatekeeper	The Commonwealth Government strategy to develop Public Key Infrastructure to facilitate Government online service delivery and e-procurement.
Hard Token	A hard token, sometimes called an "authentication token," is a hardware security device that is used to authorise a Subscriber. A common example of a hard token is a smartcard.
Identity Certificate	An identity certificate is a certificate which uses a digital signature to bind together a public key with a human identity — information such as the name of a person, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Key	A Key is a string of characters used with a cryptographic algorithm to encrypt and decrypt.
Key Custodian	A key custodian refers to the authorised person appointed to manage a key on behalf of the ATO.
Key Pair	A pair of asymmetric cryptographic Keys (e.g. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key.
Network Resource	Network Resources (devices) are units that mediate data in a computer network. Computer networking devices are also called network equipment and commonly include routers, gateways, switches, hubs, repeaters and firewalls.
National Cryptographic Authority (NCA)	The NCA of Australia is the Australian Signals Directory (ASD). ASD also maintain a list of evaluated and approved security products for use by Australian Government agencies (Evaluated Products List – EPL).
No-Lone Zone	A physically secure area which has been defined as an area which when occupied must have 2 or more trusted personnel as occupants.

Term	Definition
Non-Person Entity	An entity with a Digital ID (for example an IP address or MAC address) that acts in cyberspace, but is not a legal entity. This can include web sites, hardware devices, software applications, and information artefacts.
Modification (of certificate)	Certificate modification means the issuance of a new certificate due to changes in the information in the certificate other than the Subscriber public key. (RFC3647)
Object Identifier	An OID is a string of decimal numbers that uniquely identifies an object. These objects are typically an object class or an attribute. It serves to name almost every object type in X.509 Certificates, such as components of Distinguished Names and Certificate Policies.
Online Certificate Status Protocol (OCSP)	Method of establishing the status of a certificate that has not expired. A PKI enabled client requests the status of a certificate from an OCSP responder. The responder provides a response ("good", "revoked" or "unknown") to the client. OCSP is a more bandwidth efficient method than the download of a full Certificate Revocation List (CRL).
Operator	Any individual who is assigned keys and certificates to perform functions within the PKI. They are not regarded as either Subscribers or Relying Parties for the purposes of the ATO PKI.
PKI Operations Manager	Manages PKI operations
PKI Operator	PKI Operators perform day-to-day maintenance and support of the PKI systems managed by the ATO.
PKI Security Officer	A PKI Security Officer audits and authorises the activities of other PKI staff as they pertain to the PKI systems operated by the ATO.
Private Certificate-Signing Key	The Private Key used by the CA to digitally sign Certificates.

Term	Definition
Private Confidentiality Key	The Key used by the addressee to decrypt messages, which have been encrypted using the corresponding Public Confidentiality Key.
Private Key	The Private Key in asymmetric Key Pair that must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation, as the case may be.
Private Signing Key	A Private Key used to digitally sign messages on behalf of the relevant Subscriber.
Public Key	The Key in an asymmetric Key Pair which may be made public.
Public Key Infrastructure (PKI)	The combination of hardware, software, people, policies and procedures needed to create, manage, store and distribute Keys and Certificates based on public Key cryptography.
PKI Software	Software programs that manage digital certificate lifecycle operations and token management.
Public Key Technology	Public Key Technology is the hardware and software used for encryption, signing, verification as well as the software for managing digital Certificates.
Registration Authority (RA)	A Registration Authority (RA) is an entity that is responsible for one or more of the following functions on behalf of a CA: • Processing certificate application; • Processing requests to revoke certificates, and • Processing requests to renew, re-key or modify certificates. Processing includes the identification and authentication of certificate applicants and approval or rejection of requests. See section 1.3.2 (Registration Authorities) of this CPS and the relevant Certificate Policy (CP) for more information about the applicable RA.
Registration Officer (RO)	A person authorised by an ATO Registration Authority (RA) or ATO approved “Third party” RA to perform RA functions in accordance with this CPS, the relevant Certificate Policy and other applicable documentation.

Term	Definition
Re-Key	A Subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key. Normally used at the time of expiry of the certificate. (RFC3647)
Relying Party	A recipient of a Certificate who acts in reliance on that Certificate and/or Digital Signatures verified using that Certificate.
Renewal (of certificate)	Renewal means the issuance of a new certificate to the Subscriber without changing the Subscriber's public key or any other information in the certificate. (RFC3647). The validity period and serial number will be different in the renewed certificate.
Repository	A database of information (e.g. Certificate status, evaluated documents) which is made accessible to users including the Relying Parties.
Resource	Includes any Network Resource, Application, code, electronic service or process, Device, or data object that is capable of utilising a Certificate.
Resource Certificate	A Resource Certificate is a Certificate issued in respect of a Resource.
Revoke	To terminate a Certificate prior to the end of its operational period.
Root CA	A CA that is at the top of a certificate chain, i.e. its own certificate is self-signed.
Secure Sockets Layer	A protocol developed by Netscape for transmitting private documents via the Internet.
Subordinate CA (SubCA)	A CA which is has been established under the certificate path of the ATO Root CA. A SubCA usually issues and manages certificates to end entities. See also Operational CA.

Term	Definition
Subscriber	A Subscriber is, as the context allows: The entity whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant Certificate, and / or The person or legal entity that applied for that Certificate, and / or entered into the Subscriber Agreement in respect of that Certificate.
Subscriber Agreement	An agreement between a CA and a subscriber that establishes the rights and responsibilities of the parties regarding the issuance and management of certificates.
Superior CA	A CA which establishes/signs the certificate of a Subordinate CA.
Timestamp (trusted)	PKI based technology providing a trusted timestamp over a datum or a digital signature. A timestamp server signs a hash of the datum to be timestamped, including the correct time from a trusted time source, providing proof that the datum existed at the time of timestamping.
Token	A hardware security device containing a user's Private Key(s), and Public Key Certificate.
Transport Layer Security	A cryptographic protocol that provides security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
Trusted Role	A role conducted within a RA/CA that has access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Certificates, including operations that restrict access to a repository. Personnel who perform this role are qualified to serve in it.
Terms of use - User	myID Terms of use - User are to be viewed as a *Subscriber Agreement* and will bind the user to the Certificate Policy-User and Certificate Practise Statement and are available from the public Repository.

Term	Definition
Universally Unique Identifier	Used in computing to identify an entity or item in the format of a 128bit hexadecimal number, e.g. With a sufficiently random and generation process makes it 'practically unique' without the need for central management. See RFC4122.
Validation Authority	A Validation Authority (VA) is an entity that can perform one or more of the following functions: • Processing certificate status requests; • Validating credentials and authentication requests; • Validating signatures; and • Other services related to PKI and online authentication.
X.509 and X.509v3	The international standard for the framework for Public Key Certificates and attribute Certificates. It is part of wider group protocols from the International Telecommunication Union-T X500 Directory Services Standards.

1.6.2 Acronyms

Acronym	Definition
ADC	Australian Disputes Centre
ACSI	Australian Government Information and Communications - Electronic Technology Security Manual Instruction
ACT	Australian Capital Territory
AD	Active Directory
AGS	Australian Government Solicitor
AKR	Authorised Key Retriever
CA	Certification Authority
CAL	Certificate Assurance Level

Acronym	Definition
CAO	CA Operator
CCA	Cross-Certification Arrangement
CKMP	Cryptographic Key Management Plan
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DLM	Dissemination Limiting Marker
DN	Distinguished Name
DTA	Digital Transformation Agency
EAL	Evaluated Assurance Level
EOI	Evidence of Identity
EPL	Evaluated Products List
HSM	Hardware Security Module
I&A	Identification and Authentication
IEC	International Electro technical Commission
IETF	Internet Engineering Task Force
IP	Identity Proofing
IPR	Intellectual Property Rights
ISA	Information Systems Assurance

Acronym	Definition
ISM	Australian Government Information Security Manual
ISO	International Standards Organisation
ISP	Information Security Policy
ITSEC	Information Technology Security Evaluation Criteria
LOA	Level of Assurance
NCA	National Cryptographic Authority
NPE	Non-Person Entity
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PED	Pin Entry Device
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PKT	Public Key Technology
RA	Registration Authority
RAO	Registration Authority Operator
RFC	Request For Comment
RC	Resource Custodian

Acronym	Definition
RO	Registration Officer
SCEP	Simple Certificate Enrolment Protocol
SO	Security Officer
SRMP	Security Risk Management Plan
SSL	Secure Sockets Layer
SSP	System Security Plan
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security
TSA	Timestamp Authority
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier
VA	Validation Authority
VMP	Vulnerability Management Plan

1.6.3 References

The principal documents references by this CPS and the entities responsible for them are:

Document	Responsible Entity
The Australian Government *Protective Security Policy Framework* (PSPF)	Attorney General's Department
The Australian Government *Information Security Manual* (ISM).	Australian Cyber Security Centre

1.6.4 Conventions

In Approved Documents, unless the contrary intention appears:

- A reference to myID includes myID Certificates, Identity Tokens, or the software used by Subscribers;
- A reference to RAM includes RAM and MAS Certificates, Identity Tokens, or the software used by Subscribers;
- A reference to ATO IdP includes ATO IdP Certiicates, Identity Tokens, or the software used by Subscribers.;
- A reference to myID Operator is interchangeable with PKI Operator;
- A reference to myID Operations Manager is interchangeable with PKI Operations Manager;
- A reference to the singular includes plural and vice versa;
- Words importing a gender include any other gender;
- A reference to a person includes a natural person, partnership, body corporate, association, governmental or local authority or agency, or Device or Application or other entity;
- A reference to a document or instrument includes the document or instrument as altered, amended, supplemented or replaced from time to time;
- A reference to a section is a reference to the relevant section of that document;
- An amendment or replacement of a document does not imply any consequent amendment or alteration to any other document;
- Where a word or phrase is given a particular meaning, other parts of speech and grammatical forms of that word or phrase have corresponding meanings;
- The meaning of general words is not limited by specific examples introduced by 'including', 'for example' or similar expressions;
- The headings are for convenience only and are not to be used in the interpretation of an Approved Document; and
- Any appendix or attachment to an Approved Document (no matter how named) forms part of that document.

2 Publications and Repository Responsibilities

2.1 Repositories

The ATO operates repositories supporting the ATO PKI and its operations. Only ATO operated repositories hold authoritative ATO PKI related information (Certificates, CRLs, etc.).

The external online repository of information from the ATO PKI is accessible at the URI http://pki.ato.gov.au/. A myID webpage (https://myid.gov.au has been created to ensure all information deemed relevant to the user can be accessed in one location. This page will have a link to the ATO PKI.

2.2 Publication of Certification Information

The ATO publishes to its internal repository all CA certificates, relevant Subscriber certificates and *Certificate Revocation Lists* (CRLs). Externally, the ATO provides a repository of relevant PKI information for Relying Parties. CA Certificates, Entity Certificates, and CRLs that are not required for external use or external Relying Parties will not be published in external repositories.

The ATO provides Subscribers and Relying Parties with the URL of a website which the ATO uses to publish this CPS and relevant CPs.

2.3 Time or Frequency of Publication

The prompt publication of information in the repository is required after such information becomes available. This CPS specifies the minimum performance standards applicable to the various types of information in section 4 (Certificate Life-cycle Operational Requirements).

Public documents are published/updated promptly on approved changes.

Publication frequencies for certificates and CRLs are detailed in the applicable CP, where they differ from the minimum standards defined in this CPS.

2.4 Access Controls on Repositories

Repository information requires protection from unauthorised disclosure or modification, appropriate for the classification of the information and its value to all parties.

There are no further access controls on read-only versions of public documents.

Appropriate access controls on the repositories are used to ensure that only personnel and processes authorised by the ATO are able to write to, or modify, repository information.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Every certificate issued under this CPS:

- Must have a clear distinguishable and unique Distinguished Name (DN) in the certificate subjectName field;
- The DN will be approved by the ATO PKI System Owner;
- The Root CA's DN must be **ATO Root Certification Authority** with a Generation **[Gen]** field, comprised of G<integer> being added to each Root CA renewal; and
- The CA's DN must be **ATO Sub Certification Authority** with a Generation **[Gen]** field, comprised of G<integer> being added to each CA renewal.

For other types of names, see the relevant CP.

3.1.2 Need for Names to be Meaningful

Names used to identify the PKI core components are based on their PKI role and CA Name. Additionally, names are used to identify individual operators to allow for system auditing.

For other types of certificates, see the relevant CP.

3.1.3 Anonymity or Pseudonymity of Subscribers

See the relevant CP.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation for the ATO RCA and ATO CA certificates.

See the relevant CP.

3.1.5 Uniqueness of Names

Names are unique within the ATO PKI name space.

See the relevant CP.

3.1.6 Recognition, Authentication, and Role of Trademarks

Applicants for certificates must take all reasonable steps to ensure that subject names do not contain or comprise anything that might infringe a trade mark.

The CA will not issue a certificate where it is aware that it would contain a name that infringes (or that the CA considers might infringe) a trade mark.

Where the CA becomes aware subsequent to issuing that a name on the certificate contains or comprises anything that might infringe a trade mark (and hence has been erroneously issued), the certificate may be revoked as provided for in section 4.9 of this CPS.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Private Key generation of critical PKI core components is performed using a *Hardware Security Module (HSM)* that has undergone a security evaluation through an *Australian Signals Directorate (ASD)* recognised evaluation program. These private keys are generated internally which ensures that the private key is never exposed or accidentally released. To initiate the key generation process the CA operator must use the HSM in the presence of the required staff as dictated by the Cryptographic Key Management Plan (CKMP).

The PKI System Owner endorses all methods used to prove possession by an entity or entity owner of the private key. See the relevant CP for further details.

3.2.2 Authentication of Organization Identity

Generation of PKI core components must comply with the processes dictated in the CKMP, which indicates that the key issuing process includes:

- Identification of the infrastructure element and applicable Key Custodian;
- Witnessed generation of public and private keys;
- Generation of certificates;
- Verification by the Key Custodian that the key generation process was successful; and
- Entry into the PKI Trusted Element Register of the applicable information concerning the newly generated key.

Before issuing certificates to PKI Operators, the operator is required to undergo standard ATO on-boarding processes as detailed in the ISP, and maintain a security clearance of a minimum of NV1. In addition, the operator will need to be validated as being *affiliated* with the ATO by confirmation of their existence in the ATO Corporate Directory.

For other types of certificates, see the relevant CP.

3.2.3 Authentication of Individual Identity

Not applicable for RCA and CA certificates.

For other types of certificates, see the relevant CP.

3.2.4 Non-verified Subscriber Information

Not applicable for RCA and CA certificates.

For other types of certificates, see the relevant CP.

3.2.5 Validation of Authority

The *PKI Operations Manager* is responsible for ensuring that all PKI core components are validated in accordance with the CKMP.

For other types of certificates, see the relevant CP.

3.2.6 Criteria for Interoperation

The decision to cross certify, cross recognise, mutually recognise, at the ATO level or other form of interoperation with a third party PKI resides with the PKI System Owner and the third party.

The PKI System Owner will inspect the third party CP, and the X.509 Certificate Profiles, for compatibility and intended uses, as well as the CPS to ensure that the practice and procedures are also compatible.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The minimum identification and authentication requirements for routine re-key are as per section 3.2.2 (Authentication of Organization Identity).

For other types of certificates, see the relevant CP.

3.3.2 Identification and Authentication for Re-Key After Revocation

Re-key is not allowed after revocation for CAs.

For PKI Operators, re-key after revocation shall occur as per section 3.2 (Initial Identity Validation).

For other types of certificates, see the relevant CP.

3.4 Identification and Authentication for Revocation Requests

Revocation of certificates issued under this CPS is in accordance with this section and section 4.9.

The PKI Operations Manager, or in their absence their nominated agent, must authenticate all requests for revocation of PKI core components and the reason for revocation. Prior to revocation, the operator verifies the authority of the requestor.

The PKI System Owner must approve all request for revocation of the ATO CAs. Revocation of other PKI core components, including operator certificates, can be approved by the PKI Operations Manager or the PKI Security Officer (SO).

The revocation process provides an auditable record of this process, which includes at a minimum:

- The identity of the requestor;
- The reason for requesting revocation;
- The identity of the operator performing the revocation; and
- The issuing CA name and serial numbers of the certificates authorised for revocation, or the reason for rejecting the revocation request.

For other types of certificates, see the relevant CP.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

Creation of CAs must be authorised by the PKI System Owner.

Any individual, including both Australian Citizen and Foreign National, can submit a certificate application for either themselves or a resource (non-person entity). Suitability requirements for issuance of a certificate are detailed within the applicable CP.

4.1.2 Enrolment Process and Responsibilities

The enrolment process and responsibilities for CAs are outlined in the CA Operations Manual and CKMP.

For other certificate types, see the relevant CP.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The PKI Operations Manager must ensure that each CA creation application is in accordance with the CKMP and undergoes:

- Confirmation of approval for ATO RCA or ATO CA creation; and
- Validation of all information to be included in the certificate.

As a minimum, two delegates nominated by the PKI Operations Manager are required to witness the generation of CA keys.

The PKI Operations Manager is not required to investigate or ascertain the authenticity of any document received by them as evidence of any matter required as part of the CA creation process unless they are aware, or should reasonable be aware, that the document is not authentic or they are otherwise required to do so by law.

For other certificate types, see the relevant CP.

4.2.2 Approval or Rejection of Certificate Applications

The PKI System Owner approves or rejects CA certificate applications.

For other certificate types, see the relevant CP.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The CA shall:

- Authenticate a certificate request, to ensure that is has come from an accredited or approved source;
- Verify the request is correctly formed;
- Perform any additional process as specified in the *CA Operations Manual*.
- Compose and sign the certificate;
- Provide the certificate to the entity; and
- Publish the certificate in accordance with this CPS and relevant CP.

The certificate issue process provides an auditable record containing at a minimum:

- Details of the certificate request;
- The success, or rejection (with reason), of the certificate request; and
- The entity that submitted the certificate request.

The CA is not bound to issue keys and certificates to any entity despite receipt of an application.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

See the relevant CP.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The PKI core components are deemed to have accepted a certificate when they exercise the private key.

For other certificate types, see the relevant CP.

4.4.2 Publication of the Certificate by the CA

Certificates will be published to internal repositories. Individual CPs may have additional details.

4.4.3 Notification of Certificate Issuance by the CA to other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

There are no end entity Subscribers to this CPS. Certificate usage is defined above in section 1.4 (Certificate Usage) and as such core components, other than CAs, may only be used within the PKI.

Custodians shall protect private keys from access by other parties in accordance with the CKMP.

If the extended key usage extension is present and implies any limitation on the use of the certificate and/or private key, the CA will operate within those limitations.

For end entity certificates, see the relevant CP.

4.5.2 Relying Party Public Key and Certificate Usage

Sections 1.4 and 1.3.4 detail the Relying Party public key and certificate usage and responsibilities.

The interpretation and compliance with extended key usage attributes, and any associated limitations on the use of the certificate and/or private key, is in accordance with RFC5280.

For end entity certificates, see the relevant CP.

4.6 Certificate Renewal

The ATO RCA and ATO CA certificates cannot be renewed; however, associated core components can be renewed.

4.6.1 Circumstance for Certificate Renewal

This CPS permits certificate renewal. The minimum criterion for certificate renewals is:

- The entity has an existing approved affiliation with the ATO; and
- The new validity period will not extend beyond the approved cryptographic life of the private keys.

Certificate renewal shall not permit an operator to avoid re-key or the associated identification and authentication process.

Renewal of revoked certificates is not permitted regardless of the reason for revocation.

The relevant CP may define additional criteria.

4.6.2 Who may Request Renewal

If renewal is authorised by the relevant CP, and the parties that may request renewal are not defined in the CP, then renewal requests may be undertaken by the parties identified in section 4.1.1 (Who can Submit a Certificate Application).

4.6.3 Processing Certificate Renewal Requests

The process for CA certificate renewal is consistent with the enrolment process defined in section 4.1, however identification and authentication complies with section 3.3.

For end entity certificates, see the relevant CP.

4.6.4 Notification of New Certificate Issuance to Subscriber

For end entity certificates, see the relevant CP.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

For CA certificates see section 4.1.1.

For end entity certificates, see the relevant CP.

4.6.6 Publication of the Renewal Certificate by the CA

PKI core component renewed certificates will not be published.

For end entity certificates, see the relevant CP.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

No stipulation.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-Key

This CPS permits certificate *re-key*. Certificate re-key, rather than renewal, is the preferred process to issue a replacement certificate in the ATO PKI. Where allowed by the CP, the circumstances for certificate re-key include:

- Normal certificate expiration;
- Certificate revocation;
- Usable life of current key material has been reached; or
- Change in algorithm, or key length, required.

Loss or compromise of a current private key requires revocation.

The PKI System Owner may define other circumstances that initiate certificate re-key. When these circumstances are defined they will be published in the relevant CP.

4.7.2 Who may Request Certification of a New Public Key

Certificate re-key requests are made by an operator or the PKI System Owner.

For end entity certificates, see the relevant CP.

4.7.3 Processing Certificate Re-Keying Requests

The process for certificate re-keying is consistent with the enrolment process defined in section 4.1, however identification and authentication complies with section 3.3.

For end entity certificates, see the relevant CP.

4.7.4 Notification of New Certificate Issuance to Subscriber

The operator receives notification when a re-keyed certificate is issued, or if a certificate request for re-key is rejected.

The PKI System Owner receives notification of progress, issues, and completion of PKI System Owner initiated certificate re-keys.

For end entity certificates, see the relevant CP.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.1.1.

For end entity certificates, see the relevant CP.

4.7.6 Publication of the Re-Keyed Certificate by the CA

PKI core component re-keyed certificates will not be published.

For end entity certificates, see the relevant CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

The circumstances permitted for certificate modification include:

- Details in the certificate relevant to the Operator have changed or been found to be incorrect; and
- Interoperation with approved "Third Party" PKI, or ATO assets and systems, require certificate attributes or contents inserted, modified, or deleted.

The ATO PKI System Owner will determine other circumstances as appropriate.

For end entity certificates, see the relevant CP.

A modified Certificate is required to maintain the same level of trust and assurance as the original issued Certificate.

4.8.2 Who may Request Certificate Modification

Certificate modification for CA certificates may be requested by:

- The ATO PKI System Owner; or
- PKI Operators.

For end entity certificates, see the relevant CP.

4.8.3 Processing Certificate Modification Requests

The process for certificate modification must comply with enrolment processes defined in section 4.1. The identification and authentication procedures must comply with section 3.3.

For end entity certificates, see the relevant CP.

4.8.4 Notification of New Certificate Issuance to Subscriber

The operator receives notification when a modified certificate is issued, or if a certificate request for modification is rejected.

The ATO PKI System Owner receives notification of progress, issues, and completion of ATO PKI System Owner initiated certificate modifications.

For end entity certificates, see the relevant CP.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See section 4.4.1 (Conduct Constituting Certificate Acceptance).

4.8.6 Publication of the Modified Certificate by the CA

See section 4.4.2 (Publication of the Certificate by the CA).

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Unless otherwise stated in the relevant CP, a certificate must be *revoked* if one of the following conditions applies:

- The Subscriber notifies the CA that the original certificate request was not authorised and does not retrospectively grant authorisation.
- The Subscriber notifies the CA that the issued certificate has been compromised.
- The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the certificate suffered a key compromise or no longer complies with the requirements outlined in the CP.
- The CA obtains credible evidence any certificate it has issued has been misused.
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or other contractual or terms of use agreements that apply.
- The CA is made aware that the certificate was not issued in accordance with its CP or CPS.
- The CA determines that any of the information appearing in the certificate is inaccurate or misleading.

- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate.
- The CA obtains credible evidence of a possible compromise of a Subordinate CA's Private Key.
- Upon suspected or known loss or compromise of the media holding the Private Key.

A revoked certificate must be included on all new publications of the CRL until the certificate expires.

4.9.2 Who may Request Revocation

Revocation requests may be submitted by any of the following authorised parties:

- The PKI System Owner;
- The ATO *Information Technology Security Authority (ITSA*);
- A Law Enforcement Officer holding a valid warrant;
- A PKI Operator; or
- The Subscriber.

4.9.3 Procedure for Revocation Request

Revocation requests for PKI core components are performed by an authorised PKI Operator but must be validated by the PKI Operations Manager prior to initiation. The DRBCP details the revocation process for the ATO RCA and ATO CA in the event of an emergency.

After verification, the Operator processes the revocation request using the PKI software, which captures an auditable record of the process.

After a certificate is revoked, the CA includes the applicable certificate (certificate serial number) in the CRL that is signed by the CA and published in the repositories.

The procedure for revoking end entity certificates is set out on the relevant CP. The revocation process that applies will depend on the type of certificate being revoked.

4.9.4 Revocation Request Grace Period

For PKI core components a grace period of approximately one Operational Day is permitted. Revocation request submissions may be delayed or expedited depending on priority, or at the discretion of the ATO PKI System Owner.

The ATO PKI System Owner, or an approved delegate, in exceptional circumstances (such as security or law enforcement investigation), may approve a delay in the submission of a revocation request. An audit record of this approval is required, and must be submitted with the revocation request upon expiry of the approved delay.

For end entity certificates, see the relevant CP.

4.9.5 Time Within Which CA Must Process the Revocation Request

A CA shall process revocation requests for certificates issued under this CPS promptly after receipt.

For end entity certificates, see the relevant CP.

4.9.6 Revocation Checking Requirement for Relying Parties

Before using a certificate, the Relying Party must validate it against the CRL. It is the Relying Parties responsibility to determine their requirement for revocation checking.

4.9.7 CRL Issuance Frequency

CRLs for the ATO RCA are published when a CA is revoked or annually.

CRLs for the ATO CA under this CPS are published at intervals no longer than 7 hours.

4.9.8 Maximum Latency for CRLs

The maximum latency between the generation and publication of CRLs is 1 day.

All ATO repositories responsible for providing CRLs to Relying Parties shall be updated within the time frame specified in this CPS.

4.9.9 On-line Revocation/Status Checking Availability

Online Certificate Status Protocol (OCSP) service is not available.

The latest CRL is available from the published repositories; refer to section 2.1 (Repositories) and the certificate's CRL Distribution Point for further information.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

In the event of the need to revoke a CA certificate, if the CA is involved in any form of external recognition arrangement, the ATO will notify the relevant external parties using the "out of band" mechanisms identified in the arrangement.

4.9.12 Special Requirements re Key Compromise

See the relevant CP.

4.9.13 Circumstances for Suspension

See the relevant CP.

4.9.14 Who Can Request Suspension

See the relevant CP.

4.9.15 Procedure for Suspension Request

See the relevant CP.

4.9.16 Limits on Suspension Period

See the relevant CP.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The ATO PKI shall store in its internal repository and make available via its external web site:

- The ATO RCA and ATO CA certificates; and
- The most up-to-date CRLs.

Once a certificate has been revoked, the CA will write the certificate serial number to the CRL, which is published periodically to the PKI internal repository. While the certificate is revoked immediately after the CA processes the revocation request, any end user checking the validity of a certificate will not be able to detect the revocation until the next CRL posting or their application requires a new CRL. The details of CRL publishing frequency is documented in this CPS.

4.10.2 Service Availability

The ATO shall make this service available continuously, except for unavoidable and maintenance activities. Due to the nature of the Internet and internal ATO communications this service cannot be guaranteed to be always accessible.

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

A subscription for a certificate ends:

- When a certificate is revoked or allowed to expire; or
- When all tokens containing the certificate's matching private key have been surrendered to an RA and destroyed or zeroized in an approved manner; or
- When the PKI is terminated.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is only performed for the backup and archive of PKI core component keys. These escrow keys are permitted to facilitate key recovery in a disaster recovery situation.

The ATO PKI System Owner must approve any process that provides for the escrow, back-up, or archiving and subsequent recovery of Private Keys. See also section 6.2.3 (Private Key Escrow). Documentation of these processes is in the CA Operations Manual.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

PKI Facilities are located and constructed in accordance with ATO and Australian Government policy and legislation, for the use of:

- Systems classified up to and including the national security classification of PROTECTED; and
- The transmission, processing, and storage of national security classified PROTECTED information (electronic and hard copy).

This clause specifies the standard required, and not the classification of any systems or information. The *System Security Plan (SSP)* records the security classification of systems and information.

5.1.2 Physical Access

Physical access to PKI Facilities is in accordance with ATO and Australian Government policy and legislation, for the use of:

- Systems classified up to and including the national security classification of PROTECTED; and
- The transmission, processing, and storage of national security classified PROTECTED information (electronic and hard copy).

Access to PKI Facilities is restricted to authorised people and logged.

5.1.3 Power and Air Conditioning

All ATO facilities and contracted service provider facilities are provided with all standard building services, such as maintaining power and air conditioning, and are the responsibility of the facilities management. This includes the use of *Uninterruptible Power Supplies (UPS)*, and air conditioning to maintain ambient temperatures within equipment operating conditions and temperature threshold controls implemented on all servers.

5.1.4 Water Exposures

Protection from exposure to water is in accordance with ATO and Australian Government policy.

5.1.5 Fire Prevention and Protection

Protection and prevention from fire is in accordance with ATO and Australian Government policy.

5.1.6 Media Storage

All media is stored in accordance with ATO and Australian Government policy for the “Security Classification” of the information stored on the media.

5.1.7 Waste Disposal

Disposal of classified waste is accordance with ATO and Australian Government policy for “Product Sanitisation and Disposal”.

5.1.8 Off-site Backup

The ATO maintains off-site backups for operational services. Off-site backups are performed in accordance with the *Disaster Recovery and Business Continuity Plan (DRBCP)* and comply with ATO and Australian Government National Security Policy.

5.2 Procedural Controls

5.2.1 Trusted Roles

This CPS identifies which roles are "*Trusted Roles*". Personnel occupying trusted roles will require security clearances in accordance with the classification of the data accessed, and the *System Security Plan*.

The Trusted Roles include:

- The PKI Operations Manager;
- PKI Operators;
- myID Systems Administrators; and
- PKI Security Officer.

Each of the above positions requires access to ATO facilities. myID Systems Administrators require access to PKI services. Privilege to access these systems is controlled by the PKI Operations Manager, based on a number of factors including the risks of human error, theft, fraud, or facilities misuse. The PKI Operations Manager reserves the right to limit, restrict, or extend access privileges to PKI resources. These access privileges include to PKI rooms and facilities, network resources, and infrastructure components.

5.2.2 Number of Persons Required per Task

Administrative functions for the RCA Services (including accessing workstations, storage media, and key material) will be subject to "two party" control.

Access to operational systems by unauthorised personnel will be under the supervision of a user within the "Trusted Roles" list.

5.2.3 Identification and Authentication for each Role

Irrespective of the role or the tasks performed all access to ATO facilities and systems require identification and authentication of the individual(s) involved in accordance with the *Information Security Policy (ISP)* and SSP. Once authenticated, the appropriate facility or systems controls will determine the role, or roles, permitted for the individual(s).

The relevant CP identifies the method of identification and authentication of the end entity.

5.2.4 Roles Requiring Separation of Duties

This CPS prohibits personnel responsible for the auditing of a task to carry responsibility for the performance of that task.

The same person cannot hold the roles of PKI Operations Manager and PKI Security Officer. The same person cannot hold the roles of PKI Operator and PKI Security Officer.

The duties of each role are documented in the CA Operations Manual.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The recruitment and selection practices for PKI System personnel take into account the background, qualifications, experiences and clearance requirements of each position, which are compared against the profiles of potential candidates.

The ATO has designated that all positions supporting the PKI System are Positions of Trust and it requires that all staff working on the PKI System hold valid *Negative Vetting Level 1 (NV1)* clearances. The PKI Operations Manager must ensure those personnel hold and maintain NV1 clearances.

5.3.2 Background Check Procedures

Background checks are part of the ATO on boarding process, which is required for all ATO staff.

5.3.3 Training Requirements

All PKI System personnel will be trained in relevant policy, procedure, and technology. The PKI Operations Manager will maintain competence in all operations areas.

Specific training for the SO will focus on security management, system auditing, and system specific security applications employed in the PKI (surveillance, access systems, etc.).

PKI Operators must develop and maintain an awareness of security policies. Specific training requirements are detailed in the SSP. In general, PKI Operator personnel must complete training in:

- basic PKI concepts;
- the use and operation of the ATO CA software;
- PKI System procedures such as those described in:
  - *myID Information Security Policy,*
  - *myID Business Continuity and Disaster Recovery Plan,*
  - *myID Standard Operating Procedures, and*
  - *myID CA Operations Manual.*
- applicable privacy legislation and practices, including the *myID Privacy Policy*.
- confidentiality requirements for the protection of information, including the requirements of tax law secrecy provisions and the *Crimes Act 1914*
- computer security awareness and procedures
- the meaning and effect of this CPS and the CPs.

PKI Operations staff are encouraged to undertake training activities that will assist them to carry out their duties and improve the security and integrity of PKI operations. The PKI Operations Manager may allocate and assign staff members to any suitable training activity, such as:

- Training on the use and features of new/latest releases of PKI application software;

- Training on the use and features of new/latest releases of security tools (such as firewalls, routers, application platform security, intrusion detection systems, foot print analysis tools, backup utilities, etc.);
- Training on internal processes and procedures; and
- Training on Internet security, PKI, and similar topics conducted by Gatekeeper Evaluators, the *Australian Signals Directorate (ASD)*, the *Digital Transformation Agency (DTA)*, *the Australian Government Solicitor (AGS)*, authorised legal evaluator or private enterprises with relevant expertise.

Note that training topics must be related to the myID business plans and activities.

5.3.4 Retraining Frequency and Requirements

All PKI personnel require retraining as required to maintain currency with policy, procedure, and technology. Training on the security policy and procedures occurs annually for all trusted roles. Refer to the SSP for more information.

PKI System personnel receive a security briefing update at least once a year.

Training in the use and operation of the ATO CA and reliant application's RA's software is provided when new versions of the software are installed.

Remedial training is completed as required or when recommended by audit comments.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorised Actions

Authorised actions are identified in the Approved Documents.

The PKI Operations Manager's response to unauthorised actions is to take into account whether the misuse was an accident, omission, or malicious act.

Where a staff member has been found to have seriously misused the resources to which they have been granted access, these actions are to be documented and handled as per the *Incident Response Plan (IRP).*

Sanctions against contract employees are to be in accordance with the terms and conditions of their contract.

Depending on the nature of the actions, sanctions will comply with ATO policies for administrative or disciplinary action and may range from counselling and/or suspension of access rights, through to dismissal and/or legal action.

5.3.7 Independent Contractor Requirements

All contractors with physical or logical administrative access to ATO facilities must either have appropriate clauses in their contract or sign a Confidentiality/Non-Disclosure Agreement before they are

allowed access to PKI systems. Casual PKI Operations staff and third party access that are not already covered by an existing contract (containing the Confidentiality Agreement) may be required to sign a Confidentiality Agreement before being granted limited access to information processing facilities.

5.3.8 Documentation Supplied to Personnel

For each role, the personnel performing duties, procedures, and responsibilities receive access to the necessary documentation for that role. All documentation will be available within the ATO facilities for access by operational staff.

Access to data and reports will be subject to normal security classification controls.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Records of CA and RA infrastructure events include:

- Registration records;
- Key generation requests;
- Certificate generation requests;
- Certificate issuance records, including CRLs;
- Audit records, including security related events; and
- Revocation records.

The recorded information shall include:

- Date/time stamp;
- Event target;
- Event source;
- Event description; and
- Event status (Success/Failure).

5.4.2 Frequency of Processing Log

Audit logs are processed on a daily, weekly, monthly and annual basis. Additional processing will be performed as required if an incident occurs warranting an investigation of events leading up to the incident.

5.4.3 Retention Period of Audit Log

Backups of audit logs are retained for 12 months. Archives of audit logs are retained in accordance with *National Archive of Australia (NAA)* legislation and policy including the *Archives Act 1983 (Cth)*.

Audit retention/backup and archival policies are to ensure that together a complete record of all audit material is maintained, and recoverable, for the period specified within ATO and National Archive policy.

5.4.4 Protection of Audit Log

Protection of Audit log information is in accordance with ATO policy for the protection of security log information for systems processing up to and including PROTECTED information.

5.4.5 Audit Log Backup Procedures

Backups of audit logs occur daily.

5.4.6 Audit Collection System

The audit collection system is compliant with ATO policy for systems processing up to and including PROTECTED information.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Vulnerability assessments are in accordance with ATO policy for systems processing up to and including PROTECTED information. A Threat and Risk Assessment (TRA) and iterative security reviews have been completed for the entire myID System, in which the PKI is captured, and the findings of these are reflected in the protective measures set out in the myID SRMP.

5.5 Records Archival

5.5.1 Types of Records Archived

The ATO CA produces and stores the following data:

- Copies of issued Certificates;
- Certificate status (active or revoked);
- Copies of each issued CRL; and
- Event logs.

The myID System produces and stores the following data:

- Certificate applications requested but not yet approved;
- Certificate applications approved but not yet activated;
- Certificates issued and who approved them; and
- End user personal details.

The following audit information is archived:

- Audit logs;
- Certificate request information;
- Certificates, including CRLs generated;
- Complete back up records;
- Copies of e-mail logs;
- Formal correspondence; and
- Successive versions of this CPS and any CP.

All records archived as part of an entity's or person's interaction with the myID System will be dealt with in accordance with the requirements of the *Archives Act 1983 (Cth)*.

5.5.2 Retention Period for Archive

The retention period for archive records is in accordance with ATO and National Archive policy and relevant laws including the Archives Act 1983 (Cth). This retention period is also required for systems and applications necessary to process the archived records.

5.5.3 Protection of Archive

Archive protection occurs in accordance with ATO policy for the protection of systems processing up to and including PROTECTED information.

During copying or generation of the archive key material, the resultant media is placed into temper evident envelopes, and an entry is made in the Trusted Elements Register.

Archive key material is to be transported in accordance with ATO PROTECTED transport procedures to a facility appropriate for storage of the material.

Corresponding passphrases for archived key material are to be stored and transported separately to that of the private key.

5.5.4 Archive Backup Procedures

Archive data backup is in accordance with ATO and National Archive policies and relevant laws including the *Archives Act 1983 (Cth).*

5.5.5 Requirements for Time-Stamping of Records

Individual events shall be time stamped with the timing of the event. Audit logs shall also be time stamped with the time of archival, and if via a backup process a timestamp of the relevant backup.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

The integrity of the PKI Systems archives is verified:

- annually at the time of a programmed audit
- at any other time when a full audit is required
- at the time the archive is prepared.

5.6 Key Changeover

The PKI System ensures that the Key changeover process and procedures will provide for uninterrupted operation of the ATO CA, and will also ensure that subordinate Certificates do not become invalid as a result of ATO CA Key changeover. For that changeover, the ATO CA's Keys and Certificates are re-issued by the ATO RCA.

Key changeover periods will be in accordance with the Key Management Plan contained within the *Security Profile* and prior to normal Certificate/Key expiry.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

All security incidents are to be handled as per the SSP. Incidents are to be logged, and an investigation of the incident is to be undertaken to determine if:

- Key compromise has occurred, is suspected, or cannot be discounted;
- The incident was deliberate or accidental;
- Procedures should be modified to address the circumstances that enabled to the incident to occur; and
- Any further action is required.

If it is possible that a key compromise has occurred, the certificate requires revocation. All cross-certified CAs are to be informed if an applicable CA is compromised.

The decision to revoke the certificates subordinate to the compromised entity is optional; however the CA Operations Manual describes the necessary processes. Where a *superior* CA is compromised, ALL *subordinate* CAs are effectively revoked immediately.

The PKI System Owner receives notification of all incidents where the continued integrity of service is impacted, and will provide a formal notice to cross-certified entities, and accrediting bodies, indicating the proposed corrective action and the estimated schedule for implementation.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The DRBCP details the restoration strategy. The backup of *private signing keys* for CAs occurs only if appropriate protection applies, and is only used as part of a rebuild if compromise has not occurred or is not suspected.

5.7.3 Entity Private Key Compromise Procedures

If the entity private key is compromised it is revoked and the entity must re-apply for registration.

5.7.4 Business Continuity Capabilities after a Disaster

Priorities for Business Continuity are in the following order:

1. Physical investigation of disaster and collection of necessary evidence to complete investigation;
2. Re-establishment of secure environment for PKI operations;
3. Reconstitute the ability to issue CRLs and process revocation requests – this includes audit functionality;
4. Reconstitute the ability to receive, process and issue myIDs;
5. Return to stable operating conditions;
6. Update documentation to reflect any changes as a result of recovery – including to processes, procedures and configuration; and
7. Provide an incident closure report to all relevant authorities, including the Gatekeeper Competent Authority if requested.

5.8 CA or RA Termination

In the event of a CA or RA termination, or a CA or RA ceasing operation, its certificate requires revocation. Self-signed CAs shall follow notification procedures equivalent to key compromise. Termination of CAs, where possible, should minimise impact on subordinate certificates.

The PKI System Owner receives notification of planned and actual terminations.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key Pair generation is to be via a combination of product and process approved by the *National Cryptographic Authority (NCA)* to provide keys suitable:

- For use in PKI based authentication, non-repudiation, and integrity services for systems and data classified up to and including PROTECTED information; and
- For use in PKI based confidential communications capable of protecting symmetric (Private Key encryption) keys used to protect data up to and including UNCLASSIFIED information over publicly accessible data networks (e.g. the Internet).

Key pair generation under this CPS is in accordance with the CKMP and as such:

- Critical core components (e.g. RCA, CA) generate keys within a HSM;
- RA services generate keys within ASD recognised security evaluated software; and
- Operators generate keys using ASD recognised security evaluated software.

See the relevant CP for description on end entity key pair generation.

The CKMP details the products, process, and procedures and the approved combinations which are valid.

6.1.2 Private Key Delivery to Subscriber

Private key delivery is in accordance with the CKMP.

Private keys generated within hardware elements (HSMs) are not delivered. Soft tokens for core components are delivered direct to the PKI core component protected by a PKCS#12 file.

Private key delivery for end entities is defined in the relevant CP.

6.1.3 Public Key Delivery to Certificate Issuer

ATO RCA public keys are self generated and do not require delivery.

ATO CA public key delivery to the ATO RCA is a witnessed event, with the key being delivered via airgap in a PKCS#10 file, signed with the corresponding private key.

Other PKI core components' public keys are delivered protected within the PKI software, or delivered to the issuer in a PKCS#10 file, signed with the corresponding private key.

Private key delivery for end entities is defined in the relevant CP.

6.1.4 CA Public Key Delivery to Relying Parties

Public keys for a CA in a certificate chain for entity certificates will be accessible to Relying Parties using the approved repositories.

In addition, CA certificates in the chain which are self-signed (the "Root" CA) will be delivered using secure methods approved by the PKI System Owner to third party CAs, where a cross certification (or equivalent) agreement is in place.

6.1.5 Key Sizes

Key sizes are defined in the CKMP and relevant CP, and support SHA2 for signing and the RSA public key algorithm. The key sizes under this CPS include:

- Root CA key size = 4096 bit RSA (generated in HSM).
- CA key size = 2048 bit RSA (generated in HSM).
- RA key size = 2048 bit RSA (generated in software).
- Operator key size = 2048 bit RSA (generated in software).

6.1.6 Public Key Parameters Generation and Quality Checking

Public Key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Public Key parameters shall be generated in accordance with NCA approved guidelines.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Subscriber certificates include key usage extension fields to specify the purposes for which the keys may be used and also to technically limit the functionality of the certificate when used with X.509v3 compliant software. The correct values for key usage are set in these fields in accordance with the X.509v3 standard but ATO cannot control how third-party software applications interpret or act upon these. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of the ATO.

Key usages for CAs are specified in Appendix B.

See the relevant CP for end entity key usages.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

All cryptographic modules used are tamper resistant, tamper evident HSMs which are Common Criteria EAL 4+ certified, and FIPS 140-1, Level 3 validated.

The PKI Build and Configuration documentation details the products used.

6.2.2 Private Key (N out of M) Multi-Person Control

For ATO CA Keys, M of N is not implemented in the HSM; however cloning of the device and tokens requires presentation of two keys which are allocated to ATO trusted personnel. Further confidential details are contained in the CKMP.

6.2.3 Private Key Escrow

Escrow of end entity private authentication keys does not occur.

The relevant CP details whether private confidentiality keys are subject to escrow.

6.2.4 Private Key Backup

Back up of end entity private authentication keys does not occur, however, where the private confidentiality key is escrowed, it is backed up as part of the *System Standard Operating Procedures (SOPs).* Where such keys must be transferred to other media for backup and disaster recovery purposes, they are transferred and stored in an encrypted form protected by the HSM keys.

Critical PKI Components, such as the CA, have duplicate private keys created and archived. Where these keys are stored on hard tokens, the archive copy is also a hard token.

Duplicated hardware security tokens are recorded within tamper evident containers and signed by the PKI SO.

6.2.5 Private Key Archival

Archive of end entity private authentication keys does not occur.

Archive of PKI core component keys is permitted. Further confidential details are contained in the CKMP.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The transfer of private authentication keys from, or into, a cryptographic module does not occur except for the duplication of keys for the PKI core components. Where this occurs it is done by a product on the ASD *Evaluated Product List (EPL).*

6.2.7 Private Key Storage on Cryptographic Module

The private keys are stored in a protected are within the cryptographic module.

6.2.8 Method of Activating Private Key

Activating private keys occurs by the Key custodian authenticating into the cryptographic module. The session stays live until deactivated (see section 6.2.9).

See the relevant CP concerning a Subscriber's private key.

6.2.9 Method of Deactivating Private Key

Deactivation of private keys is in accordance with a method approved by the NCA and summarised in the relevant CP.

Private Keys stored in HSMs are automatically deactivated when the HSM is powered down or can be manually deactivated by an operator. Operator hard tokens are removed from the token reader (deactivating access) and stored in accordance with the ISP, SSP, and CKMP.

6.2.10 Method of Destroying Private Key

PKI positions of trust can destroy Private Keys. HSMs and hard tokens will be re-initialised to destroy the stored private keys.

Subscribers may destroy their own authentication Private Keys when no longer needed by securely erasing/destroying the device storing the Private Key.

6.2.11 Cryptographic Module Rating

See section 6.2.1 of this CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key archival

The CA archives all certificates it generates. CA archival is part of the archival process which requires the storage of software and hardware to allow the reconstitution of the CA if required.

The public keys of certificates are archived in accordance with section 5.5 (Records Archival).

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Within the PKI certificate lifetimes are nested and as such the key lifetime is dependent on the certificate life. In other words, an issued certificate (of an end entity or a CA) expires before the certificate of the CA that issued it. Otherwise, after the CAs expiration, the issued certificate becomes invalid, even if it has not expired.

Key lifetimes are set as a matter of policy and will depend on a number of factors, not the least of which includes the size of the key. As such the key lifetimes within the PKI are detailed in the CKMP and the applicable CP.

See Appendix B for maximum validity periods for CA certificates.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

To protect private keys, a passphrase is entered by the key custodian at the time of key generation. This passphrase is used to activate the key pair for usage.

Other passphrases and PINs used within the PKI are created by Operators at the time of installation. All passwords must comply with ATO Password Policies and the ISM.

Lifecycle management of passphrases, passwords, and PINs used in the system is in accordance with the CKMP and ATO Policy.

For end entity certificates, see the relevant CP.

6.4.2 Activation Data Protection

All passphrases used to activate the private key shall be kept in accordance with the CKMP and ATO policy.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The ATO has established an ISP and SSP for computer security technical requirements for PKI Operations. These documents carry a National Security classification and are only available to appropriately cleared personnel on a need-to-know basis.

Appropriate levels of trustworthiness and security exist throughout the PKI. Security meets ATO requirements for systems cleared to store and process data that is classified up to and including PROTECTED, which meets or exceeds the requirements mandated under Gatekeeper for a *Level of Assurance* 2 service.

Controls in place include:

- a configuration baseline and a configuration change control process;
- performance of regular and frequent systems operability tests to prove the correct operation of critical PKI components;
- strong authentication required for core PKI system access;
- role segregation;
- restrictions and controls on the use of system utilities;

- the use of monitoring and alarm systems to detect and warn of unauthorised access to computer system resources; and
- logging of all system access and use.

6.5.2 Computer Security Rating

All facilities and equipment have been constructed or selected to satisfy the requirements for a system handling or processing information classified up to and including PROTECTED. Typically, products in use within the ATO PKI have undergone a security evaluation through an ASD recognised evaluation program.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

ATO staff or contractors do not carry out any development on the COTS application source code. Development of the myID application components is only carried out in a development environment by myID developer personnel authorised to do so through formal change planning and management processes and in accordance with:

- those change planning and management processes (which include, for example, security personnel separately assessing what security measures are required, such as penetration testing and additional threat risk assessments), and
- information systems delivery and software development methodologies that apply to ATO application developments (for example myID application source code is protected by a server version control check-in check-out system, where code can only be checked out with prior authorisation, is version controlled, and can only be checked in following a peer review process).

Further information can be found in the SSP.

6.6.2 Security Management Controls

Security management controls exist to ensure that PKI systems are operating correctly and in a manner consistent with the PKI configuration baseline.

The PKI Operations Manager is responsible for maintaining the configuration baseline and for managing any changes in accordance with the SSP. The PKI Security Officer is responsible for enforcing adherence to the ATO change control processes for the PKI, and to ensure all changes to the PKI are recorded, including all hardware and software changes.

Security management controls are described in further details in the SSP.

6.6.3 Life Cycle Security Controls

No specific life cycle security ratings were sought in the development of the CA and RA software.

6.7 Network Security Controls

The ATO network security controls include:

1. Firewalls;
2. strong authentication;
3. physical access controls;
4. mechanisms to prevent denial-of-service attacks; and
5. password and other logical access controls.

The network security controls were developed after conducting a comprehensive threat and risk assessment.

The PKI System environment:

- is located, for some components, within secure physical environments which have been rated by ASIO T4 to SCEC standards;
- is located, for the remaining components, within the ASD-accredited and IRAP-assessed AWS cloud.
- is logically located behind an ASD Certified Gateway environment;
- automatically generates time-stamped logs using the system clock of the computer on which they were generated; and
- requires all persons responsible for logging information to have appropriate access in accordance with the myID Services Systems Access Register.

All successful and unsuccessful attempts to communicate with the ATO CA are logged in the ATO CA component system logs.

PKI Operation staff do not have any specific network security tasks. If they suspect a network security incident (such as a partial firewall failure) they must report it to the PKI Security Officer and the ATO ICT Service Desk.

6.8 Time-stamping

All audit log entries and transactions must be time-stamped and the asserted times shall be accurate to within +/- 5 seconds.

7 Certificate, CRL, and OCSP Profiles

Appendix B contains the formats for the certificates, and CRL profiles and formats relative to this CPS. The certificates issued under this CPS are:

- The ATO RCA;
- The ATO CA;
- Any Subordinate CA certificates signed by the ATO RCA; and
- Certificates issued to the PKI core components supporting a CA.

7.1 Certificate Profile

7.1.1 Version Number(s)

CAs operating under this CPS shall only issue X.509 Version 3 certificates.

7.1.2 Certificate Extensions

For CAs operating under this CPS, see Appendix B.

For all other certificates, see the relevant CP.

7.1.3 Algorithm Object Identifiers

Certificates under this CPS will use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Table 1 – Signature OIDs

Certificates under this CPS will use one of the following OIDs for identifying the algorithm for which the subject key was generated:

Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
Id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Table 2 – Algorithm OIDs

CAs shall only certify public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign certificates, CRLs, and any other PKI product, including other forms of revocations such as OCSP responses.

For all other certificates, see the relevant CP.

7.1.4 Name Forms

Distinguished Names (DN) shall be used by the CAs in the issuer and subject fields of the certificates. The DN shall not be blank. Names must be meaningfully related to the identity of the subscriber, except as otherwise provided in the relevant CP. Some communities or installations may choose to use other names, for example, certificates used to implement a hardware protocol where organisation identifiers are more useful. Alternate name forms may be included in the subjectAltName extension. Use of alternate name forms shall be in accordance with the CP, including criticality, types, and name constraints. The combination of DN and subjectAltName must be unique within the PKI.

The ATO RCA shall have the fixed DN subject **{CN = ATO Root Certification Authority, OU = Certification Authority, O = Australian Taxation Office, C = AU}**. The ATO RCA shall not assert the subjectAltName extension.

The ATO CA shall have the fixed DN subject **{CN = ATO Sub Certification Authority, OU = Certification Authority, O = Australian Taxation Office, C = AU}**. The ATO CA shall not assert the subjectAltName extension.

For all other certificates, see the relevant CP for name forms.

7.1.5 Name Constraints

Name constraints are not present for the ATO RCA and ATO CA certificates.

For all other certificates, see the relevant CP.

7.1.6 Certificate Policy Object Identifier

CA Certificates issued under this policy shall assert the OID **{1.2.36.1.9001.1.1.1}** for ATO RCA certificates or **{1.2.36.1.9001.1.1.1.1}** for ATO CA Certificates.

The CA certificate shall not assert OIDs representing *Levels of Assurance* of certificates issued.

For all other certificates, see the relevant CP.

7.1.7 Usage of Policy Constraints Extension

Policy constraints are not present for the ATO RCA and ATO CA certificates.

For all other certificates, see the relevant CP.

7.1.8 Policy Qualifiers Syntax and Semantics

See the relevant CP.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

See the relevant CP.

7.2 CRL Profile

7.2.1 Version Number(s)

CRLs for certificates issued under this CPS shall assert Version 2 as described in the X.509 standard [ISO9594-8].

7.2.2 CRL and CRL Entry Extensions

ATO RCA and ATO CA detailed CRL profiles covering the use of each extension are available in Appendix B.

7.3 OCSP Profile

7.3.1 Version Numbers

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessments

The infrastructure of the PKI System, including the operations of the ATO CA, requires auditing on a regular basis to ensure compliance with this CPS and all applicable CPs. The detailed process of the PKI System audits is not publicly disclosed.

In addition to the audit requirements under this CPS, Gatekeeper accreditation requires the conduct of annual audits to ensure compliance with the Gatekeeper policies and criteria (refer to https://www.dta.gov.au for Gatekeeper Compliance Audit directions).

The PKI System Owner gives further consideration to the results of such audits before possibly implementing any recommendations. The Gatekeeper CA is subject to direction by the Gatekeeper Competent Authority in relation to maintaining accreditation.

8.1 Frequency or Circumstances of Assessment

Each CA and RA requires an annual audit, more frequently if required, by an auditor appointed by the PKI System Owner to assure that they comply with this CPS and relevant CPs.

In accordance with Gatekeeper requirements, the ATO PKI must undergo an annual compliance audit.

8.2 Identity/Qualifications of Assessor

Auditors receive approval by the PKI System Owner (and where applicable, the Gatekeeper Competent Authority) based on expertise in relation to electronic signature technology, IT security procedures, or any other relevant expertise required of an evaluator to perform an evaluation properly and expertly against the Accreditation Criteria.

8.3 Assessor's Relationship to Assessed Entity

Auditors must be independent third parties and have no actual or potential conflict of interest during the period of the audit.

8.4 Topics Covered by Assessment

The purpose of audits is to ensure that PKI infrastructure elements such as each CA and RA:

- comply with accreditation criteria and policies; and
- continues to operate in accordance with the Approved Documents:

Topics covered by the assessment are based on the Gatekeeper PKI Framework, which identifies a series of compliance audit activities that must be performed to ensure the operational integrity and suitability of the infrastructure.

8.5 Actions Taken as a Result of Deficiency

Any deficiencies identified by the auditor will be documented against the audit assessment criteria in a formal written report and must be presented to the PKI System Owner. The PKI System Owner will determine actions to be taken in relation to any deficiency and will only determine corrective action after consideration of any auditor recommendations. Where the identified deficiency relates to accredited systems, authorised representatives of accrediting agencies such as the DTA and ASD will be included in reviewing results and formulating solutions.

All required corrective action must be verified to have been completed within the agreed timeframe, and failure to adequately address deficiencies identified in an audit in an agreed timeframe may result in withdrawal of accreditation.

The PKI Operations Manager, under the direction and oversight of the PKI System Owner, is responsible for the on-going management of the PKI System accreditation as a Gatekeeper accredited PKI.

8.6 Communication of Results

The results of an audit are confidential and require the auditor to communicate them only to authorised representatives of Accrediting bodies and the audited entity. Results of the compliance audit against Gatekeeper may be released at the discretion of the PKI System Owner.

All required corrective action must be verified to have been completed within the agreed timeframe.

The PKI Operations Manager has the responsibility for correspondence of results of PKI audits between the PKI and other entities, for example DTA and ASD.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

See the relevant CP.

9.1.2 Certificate Access Fees

See the relevant CP.

9.1.3 Revocation or Status Information Access Fees

See the relevant CP.

9.1.4 Fees for Other Services

No fee is levied for access to this CPS, or relevant CP, via the approved repositories. Printed copies may be made available for a fee.

See the relevant CP for any other service fees.

9.1.5 Refund Policy

Where a fee is changed for a certificate, once that certificate is issued a refund will not be provided. The relevant CA will issue a new certificate free of charge if, through the fault of the CA, an erroneous certificate was issued.

9.2 Financial Responsibility

The ATO has sufficient resources to meet its perceived obligations under this CPS. The ATO makes this service available on an 'as available' basic.

Nothing in this CPS, or relevant CP, or the issuing of Key Pairs and Certificates under it, establishes a fiduciary relationship between the ATO PKI and an end entity, or Relying Party.

The ATO PKI is not liable for any loss or damage arising from any delay or failure to perform its obligations described in this CPS. Relying Parties assume responsibility for any financial losses due to transactions authenticated using certificates issued under this CPS.

9.2.1 Insurance Coverage

See the relevant CP.

9.2.2 Other Assets

See the relevant CP.

9.2.3 Insurance or Warranty Coverage for End-Entities

See the relevant CP.

9.3 Confidentiality of Business Information

Information requires classification and handling, storing, and processing in accordance with ATO Security policy. Public Access is only to information classified as "UNCLASSIFIED".

Release of all other information will be subject to satisfying security clearance requirements and a demonstrated "need-to-know".

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The ATO PKI Privacy Notice conforms to the requirements of the *Privacy Act 1988 (Cth) (Privacy Act)* and *Information Privacy Act 2014 (ACT).* The myID Privacy Policy is available at https://www.myid.gov.au/.

No Personal Information (as defined in the *Privacy Act 1988*) will be collected during the creation of the ATO RCA or ATO CA, but it will be collected for the issuance of Operator certificates. If personal information is gathered, the collection, use, and disclosure of such information conforms to the requirements of the *Privacy Act 1988 (Cth)* (Privacy Act) and *Information Privacy Act 2014* (ACT).

9.4.2 Information Treated as Private

See the relevant CP.

9.4.3 Information Not Deemed Private

Subscribers using the ATO PKI will be required to acknowledge that Personal Information (as defined in the Privacy Act) published in the certificate may be collected, used, or disclosed as necessary for the efficient functioning of the PKI system.

Revocation of a Certificate requires publishing in the CRL in accordance with the respective CP. Revocation information is not treated as private.

The relevant CP will detail any other information that may be treated in this manner in respect of that CP.

9.4.4 Responsibility to Protect Private Information

Information collected as part of the entities' interaction with the PKI operation that is Personal Information, other than that which forms part of the *Certificate Information*, will be protected in accordance with the requirements of the Privacy Act.

Information held in the PKI can only be used by other areas within the ATO where the individual, the subject of the Personal Information, has consented or where one of the exceptions in the Privacy Act, including those in Australian Privacy Principle 6 (APP 6) apply.

Given there may be a requirement to access Personal Information as part of the verification procedure, management of the access, storage, use and disclosure of information in the PKI will be in accordance with the *Australian Privacy Principles* (APPs). Access to this information is restricted to PKI *trusted roles*.

In keeping with the requirements of the Privacy Act, the PKI implements physical and logical access control mechanisms to protect the sensitive information from unauthorised access.

The ATO encrypts communications of confidential information including the communications links between the CAs and the point of registration.

9.4.5 Notice and Consent to Use Private Information

Subscribers are to be informed of any Personal Information collected and its use and/or distribution.

Refer to relevant CP for notice and consent arrangements.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No Personal Information contained in the PKI, other than that which forms part of the Certificate Information, that relates to an identifiable ATO entity is disclosed to any external entities to the ATO unless the disclosure is in accordance with the Privacy Act (including APP 6).

ATO personnel are entitled to access Personal Information about themselves in the PKI in accordance with APP 12 of the Privacy Act. This information can be obtained by sending a signed and dated minute to the PKI Operations Centre, requesting the relevant data. The minute should include the person's full name, organisation unit and contact details and PKI staff will action the request.

Only authorised PKI staff, are permitted to access data about individual personnel. Access by these authorised persons will be in accordance with the appropriate APPs of the Privacy Act. The Privacy Commissioner has the right under the Privacy Act to conduct audits to ascertain whether Personal Information records are being maintained in accordance with the APPs.

Any ATO person is able to request changes to their own information in the PKI. Changes will, however, be subject to verification of the identity of the person requesting the change, preventing unauthorised persons from accessing or altering information.

Where changes to Personal Information (e - mail address and name) affect the contents of digital certificates, revocation and reissue of the affected certificates is required.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Unless otherwise agreed between the relevant parties:

- *Intellectual Property Rights (IPR)* in the Approved Documents, the Certificate Repository, and the CRL are owned by the ATO;
- IPR in Certificates are owned by the ATO, subject to any pre - existing IPR which may exist in the Certificates or the Certificate Information;
- the entity generating the key pairs own any IPR in the key pairs; and
- the Distinguished Names of all CAs of the ATO PKI remain the sole property of the ATO.

The IPR owners of Certificates, *Distinguished Names* and key pairs (IP Owner) grants to any other relevant entity, which has a requirement under this CPS, the CP or the other Approved Documents to

use that intellectual property, the rights it reasonably requires to perform that entity's roles, functions and obligations under this CPS, the CP or the Approved Documents.

Where an entity is required under this CPS, the CP or another Approved Document to use any software or other item owned by, or licensed to, a PKI Service Provider, that PKI Service Provider grants to the relevant entity any rights it reasonably requires to use that software or other item for the purposes of discharging that requirement.

The IPR owner warrants that:

- it has all the rights necessary to grant the licences described in this 9.5; and
- use by relevant entities of the relevant IPR pursuant to this CPS, the CP or other Approved Documents will not infringe the IPR of a third party.

The Subscriber Agreement and any other relevant documents must include intellectual property rights arrangements that are consistent with this section.

9.6 Representations and Warranties

The ATO uses this CPS, associated CPs and a Subscriber Agreement to convey conditions of usage of ATO certificates to Subscribers and Relying Parties.

Participants that may make representations and warranties include ATO CAs, RAs, Subscribers, Relying Parties, and any other participants as it may become necessary.

All parties in the ATO PKI domain, including ATO CAs and RAs and Subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will promptly notify the appropriate RA.

9.6.1 CA Representations and Warranties

The CA warrants:

- The certificate information provided to it has been accurately transcribed into the certificate;
- All other certificate information it generates itself is accurate;
- The digital certificate operates with functional key pairs; and
- That at the time it issues a certificate, the certificate contains all the elements required by the Certificate Profile as detailed in the relevant CP.

9.6.2 RA Representations and Warranties

The RA warrants the information in the certificate is true to the best of the RAs knowledge after performing identity authentication (registration) procedures with due diligence.

9.6.3 Subscriber Representations and Warranties

See the relevant CP.

9.6.4 Relying Party Representations and Warranties

Relying Parties warrant that they will:

- verify the validity of a digital certificate i.e. verify that the digital certificate is current and has not been revoked or suspended, in the manner specified in the CP under which the digital certificate was issued;
- verify that the digital certificate is being used within the limits specified in the CP under which the digital certificate was issued; and
- promptly notify the ATO PKI in the event that they suspect that there has been a compromise of the Subscriber's Private Keys.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT FOR ANY WARRANTIES EXPRESSLY GIVEN IN ACCORDANCE WITH THIS CPS OR IN A CP. NO IMPLIED OR EXPRESS WARRANTIES ARE GIVEN BY THE AUSTRALIAN TAXATION OFFICE OR BY ANY OTHER ENTITY WHO MAY BE INVOLVED IN THE ISSUING OR MANAGING OF KEY PAIRS AND/OR CERTIFICATES ISSUED UNDER THIS CPS AND ALL STATUTORY WARRANTIES ARE TO THE FULLEST EXTENT PERMITTED BY LAW EXPRESSLY EXCLUDED.

The ATO PKI uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CPS and relevant CP. However, it gives no warranty as to their full correctness. Also, the ATO PKI cannot be held responsible for any misuse of its certificate by a Subscriber or any other party in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a Relying Party.

Any Relying Party that accepts a certificate for any usage for which it was not issued does so at its own risk and responsibility.

The Subscriber Agreement must include a disclaimer that is consistent with the above disclaimer.

9.7.1 Gatekeeper Accreditation Disclaimer

The Gatekeeper Competent Authority is responsible for ensuring that the accreditation process is conducted with due care and in accordance with published Gatekeeper Criteria and Policies. The Gatekeeper Competent Authority is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Service Provider. The Digital Transformation Agency is not responsible and cannot be held liable for any loss of any kind in relation to the use of digital keys and certificates issued by a Gatekeeper accredited Service Provider. By granting a Service Provider Gatekeeper Accreditation the Digital Transformation Agency makes no representation and gives no warranty as to the:

- Accuracy of any statements or representations made in, or suitability of, the Approved Documents of a Gatekeeper accredited Service Provider;
- Accuracy of any statement or representation made in, or suitability of, the documentation of a Service Provider in a Gatekeeper recognised PKI domain; or
- Standard or suitability of any services thereby provided by any Subscriber or Relying Party or application.

9.8 Limitations of Liability

To the extent permitted by law the ATO is not liable for:

- Any use of certificates, other than uses specified in this CPS or the relevant CP;
- Falsification of transactions;
- Improper use or configuration of equipment, not operated under the responsibility of the PKI, used in transactions involving certificates;
- Compromise of private keys associated with the certificates;
- Loss, exposure or misuse of PIN code(s) etc. protecting private keys associated with the certificates;
- Erroneous or incomplete requests for operations on certificates;
- Delays arising from Force Majeure;
- The use of public or private keys of cross-certified (non - subordinate) CAs and their Relying Parties; and
- Any termination of the PKI or any related contract by the ATO.

In the absence of any documented contractual relationship between the CA and a Subscriber (other than a Subscriber Agreement) and/or Relying Party, the ATO does not accept any liability regarding the operations of the ATO PKI associated with certificates issued under this CPS.

Relevant contractual documents define any limitations to the extent of the liability of parties with regards to certificate use.

9.9 Indemnities

By using or accepting a certificate, each Subscriber and Relying Party (other than any Relying Party that is a Commonwealth non-coprate entity) agrees to indemnify and hold the ATO, as well as any of its officers, employees, agents, and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any costs or expenses of any kind, including legal fees (on a solicitor or own basis), that the ATO, as well as any of its officers, employees, agents, and contractors may incur, that are caused by the use or publication of a certificate, and that arises from that party's:

- Misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional;

- Violation of the Subscriber Agreement, Relying Party Agreement, this CPS, the relevant CP, or any applicable law;
- Compromise or unauthorised use of a Certificate or Private Key caused by the negligence of that party and not by the ATO (unless prior to such unauthorised use the ATO has received an authenticated request to revoke the Certificate);
- Use or reliance on a Certificate or Private Key; or
- Misuse of a Certificate or Private Key.

The Subscriber and its affiliated entities and individuals recognise that the ATO relies solely on the representations, warranties, undertakings and the information contained in the application (along with such other certificates, statements or documents as may be required or demanded by the ATO), to make a determination on recommending/not recommending the issuance of a digital certificate to the Subscriber and its affiliated entities and individuals and any misrepresentation thereof shall make the Subscriber and its affiliated entities and individuals liable, inter alia, for exemplary damages.

The indemnities contained herein shall be in addition to any other indemnities available generally in law or under the CPS or Subscriber Agreement and shall survive the termination of relationship between the Subscriber and the ATO, including as a result of suspension/revocation of the certificate.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments shall become effective upon publication in the Repository and will remain in effect until the notice of their termination is communicated by the ATO PKI on its web site or repository.

The CPS is available at http://pki.ato.gov.au/

9.10.2 Termination

The entire PKI may be terminated at any time by the ATO. All existing certificates, expired or unexpired, revoked, or active, will be deemed unfit for further use. The ATO is not required to revoke existing certificates in this event. All CRLs may only be used for historic or evidentiary purposes upon CA termination.

The ATO is not required to give any notice to end entities before or after CA termination, however, before the ATO PKI terminates its services, it will attempt to:

- Inform entities and subordinate RAs;
- Make widely available information of its termination; and
- Stop issuing certificates and CRLs.

In accordance with the Gatekeeper Memorandum of Agreement, the ATO will inform the Gatekeeper Competent Authority of its intention to terminate the CA and/or RA.

In the event that ATO terminates its CA operations whether voluntary or involuntary it will:

- Continue to provide the services, in particular the maintenance of a CRL or other listing of revoked digital certificates in accordance with the contractual arrangements it has with agencies, and any relevant Approved Documents which include arrangements to accommodate significant interruptions in the provision of the service.
- Co-operate with the Digital Transformation Office and other Service Providers, to achieve a seamless and secure migration of the agencies and Subscribers to a new Gatekeeper accredited CA.

9.10.3 Effect of Termination and Survival

Unless the contrary intention appears, the expiry or termination of a contractual relationship between PKI entities which imports the terms of this CPS or a relevant CP, will not affect the continued application to those entities of any provision in this CPS or a relevant CP relating to:

- Intellectual Property Rights;
- Confidential Information;
- The protection of Personal Information; or
- An indemnity; or
- Any other provision which is expressly stated to or by implication from its nature or its context is intended to continue after termination of the relevant contractual relationship.

9.11 Individual Notices and Communications with Participants

A notice or other communication (Notice) from one entity to another in relation to this CPS or a relevant CP requires signing by the sending entity. If the Notice delivery is electronic, it requires the sender's digital signature.

Notices to Organisations requires delivery to the physical, postal, facsimile or e - mail address of the Organisation, which is included in its Registration Information, or to another address, which the Organisation has specified to the sender.

Notices to Subscribers will be posted to the ATO PKI web page and where appropriate will be sent to the address within the certificate.

Unless otherwise specified in this CPS or a relevant CP, a Notice sent as required under this section is satisfied if:

- It is hand - delivered to a physical address – at the time of delivery whether or not any person is there to receive it;
- It is posted by prepaid post – at 5pm on the third day after it is posted even if the Notice is returned to the sender;
- It is transmitted by facsimile – when the sending machine produces a report showing the transmission was successful;
- It is sent by e-mail – when it enters a system under the control of the addressee; or

- By posting on the agreed web site – seven days after the date of posting.

If a Notice delivery occurs outside normal business hours at the addressee's place of business, the parties agree in these circumstances that formal receipt occurs at 9 am on the next *business day* at that place.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this CPS or a relevant CP must undergo the same procedures as for the initial approval (see section 1.5.4). Rephrasing provisions to improve their clarity as well as editorial and typographical corrections, changes to contact details are not considered amendments, however any change must be brought to the attention of the PKI System Owner and Gatekeeper Competent Authority to seek their concurrence.

9.12.2 Notification mechanism and period

The amended CPS and/or a relevant CP shall be published on the ATO PKI web site prior to it becoming effective. There is no fixed notice and comment period. Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact the parties may be changed without notice and are not subject to the notification requirements herein.

9.12.3 Circumstances under which OID must be changed

Where a CP is amended the OID for the relevant CP must be changed (editorial changes, etc., see section 9.12.1, are not amendments).

If a change in the ATO's CPS or CP is determined by the PKI System Owner to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of this CPS will also contain a revised OID for that type of certificate.

9.13 Dispute Resolution Provisions

If a dispute arises between the ATO and an employee of the Australian Taxation Office under the *Public Service Act 1999 (Cth)* (APS employee) where such dispute arises on relation to that employment relationship must be resolved through normal departmental mechanisms.

If a dispute arises between the ATO and any party other than an APS employee (Dispute), written notice must be provided so that the parties can meet to negotiate in good faith to resolve the Dispute (Dispute Notice). Should the Dispute remain unresolved 30 days after receipt of the Dispute Notice, the parties may seek mediation in accordance with the mediation rules of the *Australian Disputes Centre* (ADC), or if the ADC no longer exists, such other organisation as determined by the ATO. The mediation will be held in the *Australian Capital Territory* (ACT) and subject to the laws of the ACT. Legal representation is permissible by either party to the mediation.

Each party will bear its own costs of resolving the Dispute and the parties must bear equally the cost of any third person appointed as mediator.

Nothing in this clause prevents the ATO from preventing a party from accessing the ATO PKI, or commencing proceedings against a Subscriber for a breach of the Subscriber Agreement.

9.14 Governing Law

The governance for this CPS and any relevant CP is by, and construed to be in accordance with, the laws from time to time in force in the Australian Capital Territory.

All parties in the ATO PKI domain agree to irrevocably and unconditionally submit to the exclusive jurisdiction of the Supreme Court of the Australian Capital Territory and waive any rights to object to any proceedings brought in that court.

9.15 Compliance with Applicable Law

The ATO in operating the ATO PKI must comply with all relevant:

- Laws;
- Australian Government policies, such as the *Protective Security Policy Framework* (PSPF), *Information Security Manual* (ISM), *Gatekeeper PKI Framework* along with policies embedded within the overarching Frameworks; and,
- ATO policies, such as the ISP.

All parties to this CPS and any relevant CP must comply with all relevant Laws.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The CPS, any relevant CP and the Subscriber Agreement supersedes any prior agreements or representations, written or oral, between the parties to the Subscriber Agreement and records the entire agreement between the parties in relation to its subject matter.

9.16.2 Assignment

No party may assign its obligations or rights under this CPS, or any relevant CP, without the ATO's prior written approval.

9.16.3 Severability

If any provision of this CPS and/or relevant CP is or becomes invalid, illegal or unenforceable then that provision will, so far as possible, be read down to the extent necessary to ensure that it is not illegal, invalid or unenforceable.

If the reading down of any provision, or part of the provision, is unachievable, then the provision or part of it will be void and severable, without impairing or affecting the remaining provisions of the CPS or CP (as the case may be) in any way.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Failure by either party to enforce a provision of this CPS or any relevant CP shall not be construed as in any way affecting the enforceability of that provision or the CPS or CP (as the case may be) as a whole.

9.16.5 Force Majeure

A PKI Entity is not liable for any loss or damage arising from any delay or failure to perform its obligations described in this CPS or relevant CP if such delay is due to Force Majeure (See Appendix B).

If a delay or failure by a PKI Entity to perform its obligations is due to a Force Majeure event, the performance of that PKI Entity's obligations is suspended to the extent and for the duration caused by the Force Majeure event.

If delay or failure by a PKI Entity to perform its obligations due to Force Majeure exceeds 10 days, the PKI Entity affected by the failure to perform the obligations may terminate the arrangement, agreement or contract it has with the non - performing PKI Entity on providing notice to that Entity in accordance with this CPS or the CP.

If the arrangement, agreement or contract terminates pursuant to this section, the non - performing PKI Entity must refund any money (if any) paid by the terminating Entity to the non - performing Entity for services not provided by the non - performing PKI Entity.

9.17 Other Provisions

No stipulation.

Appendix A. Approved Certificate Policies

OID	Certificate Policy (CP)
1.2.36.1.9001.1.1.1	X.509 Certificate Policy for the **ATO Root Certification Authority (RCA)**
1.2.36.1.9001.1.1.1.1	X.509 Certificate Policy for the **ATO Subordinate Certificate Authority (CA)**
1.2.36.1.9001.1.1.7.1	X.509 Certificate Policy for the **myID User Certificates**
1.2.36.1.9001.1.1.8.1	X.509 Certificate Policy for the **myID Device Certificates**

For Point of Contact, see section 1.5.2.

Appendix B: Certificate and CRL Profiles and Formats

ATO Root CA Profile

Certificate Fields

Attribute	Value
version	"2" to indicate X.509 version 3 certificates.
issuer	Distinguished Name of the issuing CA: Common Name = ATO Root Certification Authority Organisational Unit = Certification Authority Organisation = Australian Taxation Office Country = AU
validity	20 years maximum (expressed as "From" and "To" dates)
subject	Distinguished Name of the certificate subject, in this case the Device associated with the private key. Common Name = ATO Root Certification Authority Organisational Unit = Certification Authority Organisation = Australian Taxation Office Country = AU
subjectPublicKeyInfo	The public key and the public key algorithm (RSA 4096 with a SHA-256 digest).

Certificate Extensions

Attribute	Value
Key size	4096

Attribute	Value
keyUsage [critical]	Defines valid purposes, in this case: crlSigning keyCertSigning nonrepudiation digitalSignature
certificatePolicies	CP information such as the OID and the URL where the CPS is available: Policy Identifier OID =1.2.36.1.9001.1.1.1 Certificate Practice Statement available on the Terms and Conditions page. User Notice = This certificate may only be used for the purpose permitted in the applicable Certificate Policy. Limited liability applies - refer to the Certificate Policy. Qualifier: http://pki.ato.gov.au/policy/ca.html
basicConstraints [critical]	Indicates if the subject may act as a CA and should be set to “True”. pathLengthConstraint=None
authorityInformationAccess	Access Method: 1.3.6.1.5.5.7.48.2 URL=http://pki.ato.gov.au/crls/atorootca.crt
subjectKeyIdentifier	160-bit SHA-1 hash of the value of the BIT STRING of the subjectPublicKey (Method 1 described in RFC5280).
authorityKeyIdentifier	Same value as Subject Key Identifier.

ATO CA Profile

Certificate Fields

Attribute	Value
version	“2” to indicate X.509 version 3 certificates.

Attribute	Value
serialNumber	Unique identifier for each certificate composed of randomised positive integers.
signature	Algorithm identifier for the algorithm used by the CA to sign the certificate: SHA-256 with RSA encryption.
Issuer	Distinguished Name of the issuing CA: Common Name = ATO Root Certification Authority Organisational Unit = Certification Authority Organisation = Australian Taxation Office Country = AU
validity	10 years maximum (expressed as “From” and “To” dates).
subject	Distinguished Name of the certificate subject, in this case the Device associated with the private key. Common Name = ATO Sub Certification Authority Organisational Unit = Certification Authority Organisation = Australian Taxation Office Country = AU
subjectPublicKeyInfo	The public key and the public key algorithm (RSA 2048 with a SHA-256 digest).

Certificate Extensions

Attribute	Value
Key size	2048

Attribute	Value
keyUsage [critical]	Defines valid purposes, in this case: crlSigning keyCertSigning nonRepudiation digitalSignature
certificatePolicies	CP information such as the OID and the URL where the CPS is available: Policy Identifier OID =1.2.36.1.9001.1.1.1.1 Certificate Practice Statement available on the Terms and Conditions page. User Notice = This certificate may only be used for the purpose permitted in the applicable Certificate Policy. Limited liability applies - refer to the Certificate Policy. Qualifier: http://pki.ato.gov.au/policy/ca.html
crlDistributionPoints	URL=http://pki.ato.gov.au/crls/atorootca.crl
basicConstraints [critical]	Indicates if the subject may act as a CA and should be set to “True”. pathLengthConstraint=0
authorityInformationAccess	Access Method: 1.3.6.1.5.5.7.48.2 URL=http://pki.ato.gov.au/crls/atorootca.crt
subjectKeyIdentifier	160-bit SHA-1 hash of the value of the BIT STRING of the subjectPublicKey (Method 1 described in RFC5280).
authorityKeyIdentifier	Same value as ATO Root CA Subject Key Identifier.

ATO Root CA CRL Profile

CRL Attributes

Attribute	Value
CRL issue period	A new CRL is issued each time the Root CA is brought online to renew the Australian Taxation Office CA CRL.
CRL validity	1 year.
CRL signature digest	SHA-256
revokedCertificates	List of revoked certificates by serial number.
reasonCode	Not included in the CRL.
invalidityDate	Date at which it is known or suspected that the private key was compromised or that the certificate should otherwise be considered invalid.

ATO CA CRL Profile

CRL Attributes

Attribute	Value
CRL issue period	1.5 hours.
CRL validity	7 hours.
CRL signature digest	SHA-256
revokedCertificates	List of revoked certificates by serial number.
reasonCode	Not included in the CRL.

Attribute	Value
invalidityDate	Date at which it is known or suspected that the private key was compromised or that the certificate should otherwise be considered invalid.