Australian Government
Australian Taxation Office

Certificate Policy - myID User

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	5 November 2024	myID review & update

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 is the Certificate Policy (CP) for ATO PKI certificates that are issued to individuals for personal and business use within the myID systems context.

This CP should be read in conjunction with:

- The ATO PKI X.509 Certification Practice Statement (CPS)
- The myID Terms of use - User

This CP identifies the rules to manage the myID User certificates, including the obligations of PKI entities and how they are used. It does not describe how to implement these rules as that information is in the CPS or documents referenced by the CPS. In general, the rules identify the minimum standards in terms of performance, security and/or quality.

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

A document hierarchy applies within the documents governing this Public Key Infrastructure:

- The provisions of the Terms of Use – User or other relevant contract override the provisions of this CP
- The provisions of this CP override the CPS.
- The provisions of the CPS govern any matter on which this CP is silent.

1.1 Overview

A myID User Certificate is issued to an individual who is establishing an identity with the Commonwealth's Digital Identity Provider, myID, operated and managed by the Australian Taxation Office (ATO).

Once the individuals identity is established the certificate is used as part of authenticating their identity for authenticated access to participating organisations (Relying Parties) online services via the myID system.

Not all Relying Parties, or transactions, within the identity federation will require the same level of confidence in the digital identity. As such, Relying Parties will require varying levels of confidence (accepted risk) in the digital identity based on the consequence of incorrectly identifying a person in the provision of their services. Therefore, whilst the myID User Certificate is provided to the individual after the user has validated their email during the enrolment process it includes a Proof of Identity (POI) identifier that uniquely identifies the User within myID systems. This POI, in combination with the

certificate, enables the myID system to establish the required proof of identity required for the Identity Proofing (IP) level[1] required by the Relying Party.

No authority, or privilege, applies to an individual that is issued a myID User Certificate, other than confirming the person 'owns' the digital identity being presented; thereby enabling the administrator of the resource/service to make access/authorisation decisions based on their systems policies for the digital identity.

1.2 Document Name and Identification

This document is known as the *Certificate Policy - myID User*. It is identified by the *object identifier* (OID) 1.2.36.1.9001.1.1.7.1, based on the following structure:

1	ISO code
2	Member Body
36	Australia
1	Government
9001	Whole of Government AUSid
1	Australian Taxation Office Root CA (RCA)
1	Australian Taxation Office Sub CA (CA)
7	myID User Certificate Policy
1	Version number

1.3 PKI Participants

1.3.1 Certification Authorities

The Certification Authorities (CAs) that issue certificates under the CP are Gatekeeper accredited CAs subordinate to the ATO Root CA (ATO RCA).

1.3.2 Registration Authorities

The *Registration Authorities* (RAs) that perform the registration function under this CP are Gatekeeper and TDIF accredited RAs. For further information, see the CPS.

1.3.3 Subscribers

A *Subscriber* is defined as follows:

- The entity (an individual person) whose unique myID System identifier appears within the "Subject Distinguished Name" on the relevant Certificate.

[1] For information on the respective Identity Proofing Levels refer to Trusted Digital Identity Framework (TDIF) Identity Proofing Requirements https://www.dta.gov.au/our-projects/digital-identity/join-identity-federation/accreditation-and-onboarding/trusted-digital-identity-framework)

Subscribers in this context include any individual who has been approved as having a requirement to be authenticated to the myID System and who has validated their email address.

A Subscriber issued a certificate under this CP does not automatically receive access, authority, or privilege to assets or systems owned or managed by the ATO or by other relying party within the myID community of interest.

1.3.4 Relying Parties

See CPS.

1.3.5 Other Participants

See CPS.

1.4 Certificate Usage

Certificates issued under this CP, in conjunction with their associated Private Keys, assist a Subscriber in Authenticating themselves to a Relying Party within the myID community of interest electronically in online transactions.

Note that because the Subscriber's identity has not been verified when the certificate is issued to that Subscriber (and only the email address has been verified), use of a certificate is necessary - but is usually not sufficient on its own - to authenticate a user for the purposes of carrying out a myID transaction.

That is, the certificate is one part only of the Subscriber's myID credential. The other parts of of that myID credential will depend on the level of identity proofing that the user has carried out. Please refer to 3.2.3 (Authentication of Individual Identity)

1.4.1 Appropriate Certificate Uses

Certificates issued under this CP, in conjunction with their associated *Private Keys*, may be used:

- For the authentication of the identity of a Subscriber, during the conduct of any lawful business with that individual, as an individual associated with the myID System.
- To verify the integrity of a communication from a Subscriber to a myID Relying Party.

1.4.2 Prohibited Certificate Uses

Any kind of unlawful or improper use of an myID User Certificate is prohibited. This includes conducting transactions that are illegal or unethical.

The acceptance of a certificate by a Relying Party for anything other than an explicitly approved purpose is at the Relying Party's own risk. The ATO disclaims any and all liability in such circumstances.

1.5 Policy Administration

1.5.1 Organization Administering the Document

See CPS.

1.5.2 Contact Person

See CPS.

1.5.3 Person Determining CPS Suitability for the Policy

See CPS.

1.5.4 CPS Approval Procedures

See CPS.

1.6 Definitions and Acronyms

Acronyms and terms used in this CP are defined in the CPS. Note that the defined terms in this CP 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.

2 Publications and Repository Responsibilities

2.1 Repositories

See CPS.

2.2 Publication of Certification Information

The ATO publishes Subscriber certificates, the issuing CA certificate and the issuing CA's latest *Certificate Revocation List* (CRL) in its repository. This information is available to Relying Parties internal and external to the ATO.

The ATO provides for Subscribers and Relying Parties the URL of a website that the ATO uses to publish:

> This CP; and

> The CPS.

2.3 Time or Frequency of Publication

Published documentation is updated on approved change.

The issuing CA publishes new certificates and CRLs at least once every week.

2.4 Access Controls on Repositories

See CPS.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Every certificate issued under this CP:

- Must have a clear, distinguishable, and unique *Distinguished Name* (DN) in the certificate subjectName field;
- Must have common name components of the name that are unique to the individual within the myID System.

The DN is in the form of a X.501 printable string and is not blank.

3.1.2 Need for Names to be Meaningful

Names used to identify the Subscriber are to be based on the Subscriber's *Proof of Identity* (POI) identifier and relate to identity of the Subscriber as provided by the myID Identity System.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

Names are unique within the myID System. Names used in certificates are unique to the individual's record in the myID Identity System and valid for that individual irrespective of their affiliation to the ATO. A name issued to an individual is permanent, even after the Subscriber's affiliation expires, and this CP prohibits the re-use of that name by another individual as a Subscriber name.

3.1.6 Recognition, Authentication, and Role of Trademarks

See CPS.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The initialisation of the myID registration process for an Individual initiates the certificate issuance.

A soft token containing the *key pair* is generated for the individual on the device the first time the user interacts with the myID System. To prove possession of the private key, a digitally-signed certificate request is submitted to the RA.

3.2.2 Authentication of Organization Identity

To be identified as *affiliated* with the myID System, the Subscriber must be registered in the myID Identity Management Service. This identification is validated by aligning their unique identifier during the enrolment process.

3.2.3 Authentication of Individual Identity

A myID User certificate is provided to the individual after the user has validated their email during the initial stage of the enrolment process. This certificate includes a Proof of Identity (POI) identifier that uniquely identifies the User within myID systems. This POI, in combination with the certificate, enables the individual to authenticate to the myID system to complete the enrolment process and proof their identity to the required level of assurance.

Until the individual completes the enrolment they cannot be authenticated to Relying Parties as the minimum Identity Proofing level currently within the identity federation is Identity Proofing (IP) 2, which includes verification of TDIF approved commencement of identity or photo identity documents and use in the community document(s).

See https://myID.gov.au for further information regarding the authentication of individuals.

3.2.4 Non-verified Subscriber Information

All Subscriber information contained in a certificate is verified against the myID Identity Management Service.

3.2.5 Validation of Authority

Applicants must be registered as a user within the myID Identity Management Service for validation.

3.2.6 Criteria for Interoperation

See CPS.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

No additional identification is required for routine *re-key*. Activation of a valid Private Key in interaction with the myID System automatically generates a routine re-key, where applicable.

3.3.2 Identification and Authentication for Re-Key After Revocation

See section 3.2.

3.4 Identification and Authentication for Revocation Requests

Certificates issued through the myID System are normally not revoked, unless compromise occurs.

If an associated device hosting a certificate is unregistered or revoked from the myID System, then the certificate contained within will revoked.

If a Subscriber knows or suspects that their device has been compromised, they must contact ATO myID support immediately.

See section 4.9 in this CP and the CPS for more information on revocation.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

An individual who has submitted an application for a certificate within the myID System and validated their email address will be issued a myID certificate.

Note this is usually not sufficient to participate in the myID system as a credential holder who carries out transactions with myID relying parties. Usually, the Subscriber will be required to carry out further identity proofing to gain a myID credential that allows them to carry out transactions within the myID system. See 3.2.3 (Authentication of Individual Identity)

Once the applicant has instantiated the myID application on their device, and entered their email address, the initial attempt at registration into the myID System initiates the certificate application process. This process is automated.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

See section 3.2.3.

4.2.2 Approval or Rejection of Certificate Applications

All requests that meet the conditions of the Certificate Policy requirements will be approved and passed to the RA; others are rejected.

The RA signs and forwards the certificate request to the CA. The CA only certifies certificate requests that are signed by an approved RA.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

See CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Subscriber registration process returns the issued certificate directly to the Subscriber's application storage on the device from which the Subscriber initiated the application. There is no other notification.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber is deemed to have accepted the certificate when they have *exercised* the private key. This usually occurs when the Subscriber uses the myID application to initiate their identity proofing checks.

4.4.2 Publication of the Certificate by the CA

The ATO CA publishes all certificates to its internal repository.

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

Subscriber private key and certificate usage is defined above in section 1.4. Subscriber responsibilities are described below in section 9.6.3.

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

4.5.2 Relying Party Public Key and Certificate Usage

Section 1.4 and 1.3.4 detail the Relying Party's 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.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

This CP permits certificate renewal.

Cetificates are renewed automatically when the certificate is nearing expiry, when the user authenticates with their myID credential.

4.6.2 Who may Request Renewal

See section 4.1.1.

4.6.3 Processing Certificate Renewal Requests

The process for certificate renewal is consistent with the enrolment process defined in section 4.1. The identification and authentication procedures must comply with section 3.3.

4.6.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See section 4.4.2.

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

Certificate re-key is the process of generating a new key pair and issuing a new certificate that certifies a new public key. All myID User Certificate renewals include re-keying.

See CPS more information.

4.7.2 Who may Request Certification of a New Public Key

Certificate re-key may be requested by the:

- myID System Owner; or
- the Subscriber, as part of initiating the renewal process.

4.7.3 Processing Certificate Re-Keying Requests

The process for certificate re-key is consistent with the enrolment process defined in 4.1. The identification and authentication procedures must comply with 3.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

See section 4.2.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificate modification is not supported by the myID System. If a certificate needs to be modified, it will be re-keyed.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

See CPS.

4.9.2 Who may Request Revocation

Revocation of a myID User Certificate may be requested by the myID RA, in addition to parties stipulated in the CPS.

4.9.3 Procedure for Revocation Request

Where used, revocation requests received by the ATO will be processed by the ATO *PKI Operators*. These requests are to be verified on receipt in accordance with section 3.4 and processed in priority order

After verification the PKI Operator processes revocation requests by using the PKI software, which captures an auditable record of the process. This usually involves having the RA authenticate to the CA to submit the request.

After the 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.

4.9.4 Revocation Request Grace Period

A grace period of approximately one *Operational Day* from receipt of the revocation request is permitted. Regardless of any grace period, revocation request submissions may be delayed or expedited depending on priority, or at the discretion of the myID System Owner.

The myID System Owner, or an approved delegate, in exceptional circumstances (such as a 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.

4.9.5 Time Within Which CA Must Process the Revocation Request

A CA shall process revocation requests for certificates issued under this CP promptly after receipt (taking the grace period and action takening exceptional circumstances as provided in section 4.9.5 into account)

4.9.6 Revocation Checking Requirement for Relying Parties

Before using a certificate the Relying Party should validate it against the CRL. It is the Relying Party's responsibility to determine their requirement for revocation checking ensuring that the time period in which revocation can occur is taken into account. Revocation request submissions.

Certificates issued under this CP are unsuitable for a Relying Party's use if the revocation checking conflicts with any provisions of isection 4.9.

4.9.7 CRL Issuance Frequency

See CPS.

4.9.8 Maximum Latency for CRLs

See CPS.

4.9.9 On-line Revocation/Status Checking Availability

This CP does not support OCSP.

The latest CRL is available from the published repositories; refer to section 2.1 and the certificates 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

See CPS.

4.9.12 Special Requirements re Key Compromise

No stipulation

4.9.13 Circumstances for Suspension

This CP does not support certificate suspension.

4.9.14 Who Can Request Suspension

This CP does not support certificate suspension.

4.9.15 Procedure for Suspension Request

This CP does not support certificate suspension.

4.9.16 Limits on Suspension Period

This CP does not support certificate suspension.

4.10 Certificate Status Services

See CPS.

4.11 End of Subscription

See CPS.

4.12 Key Escrow and Recovery

Escrow, backup, and archiving of private keys issued under this CP is not permitted. See the CPS for escrow requirements as these relate to the CA.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

See CPS.

5.2 Procedural Controls

See CPS.

5.3 Personnel Controls

See CPS.

5.4 Audit Logging Procedures

See CPS.

5.5 Records Archival

See CPS.

5.6 Key Changeover

See CPS.

5.7 Compromise and Disaster Recovery

See CPS.

5.8 CA or RA Termination

See CPS.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Subscriber keys are generated on the Subscriber's device during the requesting process.

6.1.2 Private Key Delivery to Subscriber

The key generation is performed on the Subscriber's device and stored directly on the Subscriber's application local storage, so no delivery is required.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber's public key is provided to the CA in a PKCS#10 certificate request file signed with the corresponding private key.

6.1.4 CA Public Key Delivery to Relying Parties

See CPS.

6.1.5 Key Sizes

The key sizes under this CPS include:

> Subscriber key size = 2048 bit RSA (generated in software).

6.1.6 Public Key Parameters Generation and Quality Checking

See CPS.

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

Subscriber key and certificate usage is defined above in section 1.4.

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. 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 PKI.

See Appendix A.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Subscriber keys are stored in the Subscriber's device certificate store, protected by a passphrase known only by the Subscriber.

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

No stipulation.

6.2.3 Private Key Escrow

Escrow of private keys issued under this CP is not permitted.

6.2.4 Private Key Backup

No stipulation.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

No stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Key

To activate the private key, the Subscriber must provide a passphrase to the application hosting the key pair, which is used to decrypt the private key and provide the Subscriber access to it.

6.2.9 Method of Deactivating Private Key

The Subscriber's private key will be deactivated when they complete the authentication process with the myID System, or if they close the application.

6.2.10 Method of Destroying Private Key

The Subscriber's private key will be destroyed if:

- The Subscriber deletes the application hosting the private key from their device; or
- The private key is re-keyed.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key archival

See CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Subscriber certificate has a maximum validity period of 2 years to limit the key lifetime. For further information, see CPS.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No stipulation.

6.4.2 Activation Data Protection

All passphrases used to activate the private key are known only to the Subscriber.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

See CPS.

6.6 Life Cycle Technical Controls

See CPS.

6.7 Network Security Controls

See CPS.

6.8 Time-stamping

See CPS.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

All certificates are X.509 Version 3 certificates.

7.1.2 Certificate Extensions

See Appendix A.

7.1.3 Algorithm Object Identifiers

Certificates under this CP 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 CP 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.

7.1.4 Name Forms

The Subject Name component is based on the Subscriber's POI ID and generated UUID and defined as **{CN = <POI ID>, dnQualifier = <UUID>, O = mygovid.gov.au, C = AU}**. It is encoded as an X.501 printable string where possible, and using UTF-8 otherwise.

7.1.5 Name Constraints

Name constraints are not present.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy shall assert this CP's OID: **{1.2.36.1.9001.1.1.7.1}**

7.1.7 Usage of Policy Constraints Extension

Policy constraints are not present.

7.1.8 Policy Qualifiers Syntax and Semantics

The only policy qualifiers that are permitted are the CPS Pointer qualifier and the User notice qualifier.

The CPS Pointer, if used, shall contain a HTTP URI link to the *Certification Practice Statement* (CPS) published by the CA, or to a webpage from which the CPS can then be downloaded.

The User notice, if used, shall only contain the explicitText field.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

This CP does not require the certificate policies extension to be critical. Relying Parties whose client software does not process this extension do so at their own risk.

7.2 CRL Profile

7.2.1 Version Number(s)

CRLs issued shall be X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

See Appendix A.

7.3 OCSP Profile

7.3.1 Version Numbers

No stipulation.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audits and Other Assessments

8.1 Frequency or Circumstances of Assessment

See CPS.

8.2 Identity/Qualifications of Assessor

See CPS.

8.3 Assessor's Relationship to Assessed Entity

See CPS.

8.4 Topics Covered by Assessment

See CPS.

8.5 Actions Taken as a Result of Deficiency

See CPS.

8.6 Communication of Results

See CPS.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

There is no fee for accessing Certificates from approved repositories.

9.1.3 Revocation or Status Information Access Fees

There is no fee for accessing the CRL from approved repositories.

9.1.4 Fees for Other Services

See CPS.

9.1.5 Refund Policy

See CPS.

9.2 Financial Responsibility

See CPS.

In addition, certificates issued under this CP do not contain, or imply, and authority, access, or privilege. Relying Parties assume responsibility for any financial limit they wish to apply for transactions authenticated using certificate issued under this CP.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

See CPS.

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://myid.gov.au.

In order to provide an audit and evidentiary trail of the verification process, and documentation presented to confirm an individual's identity, the ATO is required to collect Personal Information (as defined in the *Privacy Act 1988* (Cth)). The collection, use, and disclosure of such information is governed by the *Privacy Act 1988* (Cth) and the *Information Privacy Act 2014* (ACT).

At enrolment, applicants agree to the terms and conditions of being given an account on the myID System, acknowledging that the ATO may collect, use, or disclose Personal Information about them, for the purposes discussed below.

9.4.2 Information Treated as Private

Personal Information is not published in the digital Certificate and will be treated as private. The ATO PKI relies on the Subscriber being provisioned an account within the myID System. Refer to the myID Privacy Policy for further information.

9.4.3 Information Not Deemed Private

See CPS.

9.4.4 Responsibility to Protect Private Information

See CPS.

9.4.5 Notice and Consent to Use Private Information

Refer to the myID Privacy Policy and Terms and Conditions at https://myid.gov.au.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See CPS.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

See CPS.

9.6 Representations and Warranties

See CPS.

9.6.1 CA Representations and Warranties

See CPS.

9.6.2 RA Representations and Warranties

See CPS.

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

See CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

See CPS.

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

See CPS.

In addition, the Gatekeeper Competent Authority is only responsible for performing the accreditation process with due care, in adherence to published Gatekeeper Criteria and Policies. The Digital

Transformation Agency is not liable for any errors and/or omissions in the final *Approved Documents*, which remain the responsibility of the myID System Owner.

9.9 Indemnities

See CPS.

9.10 Term and Termination

9.10.1 Term

This CP 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.

9.10.2 Termination

See CPS.

9.10.3 Effect of Termination and Survival

See CPS.

9.11 Individual Notices and Communications with Participants

See CPS.

9.12 Amendments

See CPS.

9.13 Dispute Resolution Provisions

See CPS.

9.14 Governing Law

See CPS.

9.15 Compliance with Applicable Law

All parties to this CP must comply with all relevant Subscriber and/or relying party agreements, in addition to those stipulated in the CPS.

9.16 Miscellaneous Provisions

See CPS.

9.17 Other Provisions

See CPS.

Appendix A: Certificate Profiles and CRL Profiles and Formats

myID User Certificate Profile

Certificate Fields

Attribute	Value
version	"2" to indicate X.509 version 3 certificates.
serialNumber	Unique identifier for each certificate, composed of incremental 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 Sub Certification Authority OU = Certification Authority Organisation = Australian Taxation Office Country = AU
validity	2 years maximum (expressed as "From" and "To" dates)
subject	Distinguished Name of the certificate subject, in this case the User associated with the private key. CN = <POI ID> dnQualifier = <UUID> O = mygovid.gov.au C = AU

Attribute	Value
subjectPublicKeyInfo	The public key and the public key algorithm (RSA 2048 with a SHA-256 digest).

Certificate Extensions

Attribute	Value
Key size	2048
keyUsage **[critical]**	Defines “valid purposes”, such as encipherment or signature, for the key contained in the certificate. Settings are: - Digital Signature - Non-Repudiation - Key Encipherment - Data Encipherment The values keyCertSign or crlSign are not allowed in User Certificates. See section 4.4 above for more information on valid usage of the single key pair.

Attribute	Value
certificatePolicies	CP information such as the OID and the URL where the CPS is available: [1]Certificate Policy: Policy Identifier=1.2.36.1.9001.1.1.7.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Use this certificate only for the purpose permitted in the applicable Certificate Policy. Limited liability applies - refer to the Certificate Policy. [2]Certificate Policy: [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS 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 “False”. pathLengthConstraint=None
cRLDistributionPoints	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pki.ato.gov.au/crls/atosubca.crl
extendedKeyUsage	Defines additional valid purposes for the key contained in the certificate: clientAuthentication

Attribute	Value
authorityInformationAccess	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://pki.ato.gov.au/crls/atosubca.crt

CRL Profile

See CPS.