



Australian Government
Australian Taxation Office

myGovID Certificate Policy - Machine

myGovID System

Version 1.0

September 2019

Contents

1	Introduction	5
1.1	Overview	5
1.2	Document Name and Identification	5
1.3	PKI Participants	6
1.4	Certificate Usage	7
1.5	Policy Administration	7
1.6	Definitions and Acronyms	8
2	Publications and Repository Information	9
2.1	Repositories	9
2.2	Publication of Certification Information	9
2.3	Time of Frequency of Publication	9
2.4	Access Controls on Repositories	9
3	Identification and Authentication	10
3.1	Naming	10
3.2	Initial Identity Validation	10
3.3	Identification and Authentication for Re-key Requests	11
3.4	Identification and Authentication for Revocation Requests	11
4	Certificate Life Cycle Operational Requirements	13
4.1	Certificate Application	13
4.2	Certificate Application Processing	13
4.3	Certificate Issuance	14
4.4	Certificate Acceptance	14
4.5	Key Pair and Certificate Usage	14
4.6	Certificate Renewal	16
4.7	Certificate Re-Key	16
4.8	Certificate Modification	17
4.9	Certificate Revocation and Suspension	17
4.10	Certificate Status Services	19
4.11	End of Subscription	19
4.12	Key Escrow and Recovery	19
5	Facility, Management, and Operational Controls	20

5.1	Physical Controls	20
5.2	Procedural Controls	20
5.3	Personnel Controls	20
5.4	Audit Logging Procedures	20
5.5	Records Archive	20
5.6	Key Changeover	20
5.7	Compromise and Disaster Recovery	20
5.8	CA or RA Termination	20
6	Technical Security Controls	21
6.1	Key Pair Generation	21
6.2	Private Key Protection and Cryptographic Module Engineering Controls	22
6.3	Other Aspects of Key Pair Management	23
6.4	Activation Data	23
6.5	Computer Security Controls	23
6.6	Life Cycle Technical Controls	23
6.7	Network Security Controls	24
6.8	Time-stamping	24
7	Certificate, CRL and OCSP Profiles	25
7.1	Certificate Profile	25
7.2	CRL Profile	26
7.3	OCSP Profile	26
8	Compliance Audits and Other Assessments	27
8.1	Frequency of Circumstances	27
8.2	Identity/Qualifications of Assessor	27
8.3	Assessor's Relationship to Assessed Entity	27
8.4	Topics Covered by Assessment	27
8.5	Actions Taken as a Result of Deficiency	27
8.6	Communication of Results	27
9	Other Business and Legal Matters	28
9.1	Fees	28
9.2	Financial Responsibility	28
9.3	Confidentiality of Business Information	28
9.4	Privacy of Personal Information	28
9.5	Intellectual Property Rights	29
9.6	Representations and Warranties	29
9.7	Disclaimers of all other Warranties	29
9.8	Limitation of Liability	30

9.9	Indemnities	30
9.10	Term and Termination	30
9.11	Individual Notices and Communications with Participants	31
9.12	Amendments	31
9.13	Dispute Resolution Procedures	31
9.14	Governing Law	31
9.15	Compliance with Applicable Law	31
9.16	Miscellaneous Provisions	31
	Appendix A: Certificate Profiles and CRL Profiles and Formats	32

1 Introduction

This is the Certificate Policy (CP) for myGovID certificates that are issued to machines for personal and business use within the myGovID systems. Please refer to Section 1.3.3.1 for a definition of Machines context.

This CP should be read in conjunction with:

- > The myGovID Certification Practice Statement (CPS)
- > The myGovID Terms of use - Machine

This CP identifies the rules to manage the ATO myGovID Machine 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 – Machine 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 myGovID Machine Certificate is issued to a machine which is establishing an identity with the Commonwealth's Digital Identity Provider, myGovID, operated and managed by the Australian Taxation Office (ATO).

Once the machines identity is established the certificate is used as part of authenticating its identity for authenticated access to participating services utilising the myGovID system.

1.1.1 Community of Interest

See CPS section 1.1.1.

1.1.2 Document Hierarchy

A document hierarchy applies: the provisions of the Terms of Use or other relevant contract override the provisions of this CP, and the provisions of this CP override the CPS.

1.2 Document Name and Identification

This document is known as the *Machine Certificate Policy*. It is identified by the object identifier (OID) 1.2.36.1.9001.1.1.8.1, 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)
8	Machine Certificate Policy
1	Version number

1.3 PKI Participants

1.3.1 Certification Authority

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

See CPS section 1.3.1.

1.3.1.1 ATO Certification Authority (ATO CA)

See CPS section 1.3.1.2.

1.3.2 myGovID Registration Authority (myGovID RA)

See CPS section 1.3.2.

1.3.3 Subscribers

Machine certificates are only issued to non-person entities. See CPS section 1.3.3

1.3.3.1 Machines

A Machine is computer hardware (such as a server) onto which a Machine Certificate may be installed. For a myGovID Machine Certificate, the Machine on which it installed must be owned, controlled, and/or operated by the organisation/individual identified in that Certificate.

1.3.4 Relying Parties

See CPS section 1.3.4.

1.3.5 Other Participants

See CPS section 1.3.5.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

The appropriate use of a myGovID Machine Certificate is limited to authenticating the Machine identified in that Certificate as owned, controlled and/or operated by the Organisation identified in that Certificate for the purposes of a machine-to-machine interaction between that Organisation and an entity within the myGovID COI.

1.4.2 Limits on Use

A myGovID Machine Certificate is designed for the Organisation identified in that Certificate to authenticate itself, and that it owns, controls and/or operates the Machine identified in that Certificate, for the purposes of carrying out a machine-to-machine interaction with an entity within the myGovID COI. The myGovID System does not support use of myGovID Machine Certificates by or with any other relying parties. Any person who uses, or relies on, a myGovID Machine Certificate in any other circumstances does so at their own risk and responsibility.

Note: a myGovID does not provide any indication of the level of authority, delegation or privileges that the myGovID Holder may possess, and is for authentication rather than authorisation purposes.

For other limits on use, refer to the *Certification Practice Statement* and *myGovID Terms of Use - Machine*

1.4.3 Prohibited Certificate Uses

Any kind of unlawful or improper use of a myGovID Machine Certificate is prohibited. 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. See CPS section 1.4.2

1.5 Policy Administration

See CPS section 1.5.

1.6 Definitions and Acronyms

Acronyms and terms used in this CP are defined in the CPS, unless they are otherwise defined in the table below. Defined terms may be upper or lower case.

Term	Definition
Organisation	A legal entity that has, or is entitled to have, an ABN
Organisation Associate	An individual who can exercise the powers of the relevant Organisation (and to authorise others to act on their behalf)
Administrator	A general term for an external person formally appointed to manage a company or its property
Machine Credential Administrator (MCA)	Role of nominated individual by the Organisation who has a myGovID credential to IP2 Level of Assurance 2 in accordance with published Gatekeeper Criteria and Policies.
Relationship Authorisation Manager(RAM)	ATO website to manage Organisation authorisation: https://info.authorisationmanager.gov.au/

See CPS section 1.6.

2 Publications and Repository Information

2.1 Repositories

See CPS Section 2.1.

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 of 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 section 2.4

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Every Certificate issued under this CP must have a Distinguished Name (DN) that is unique to the subject of the Certificate and compliant with the X.501 standard. The DN must be in the form of a X.501 printable string and may not be blank. The DN must be unique within the context of the PKI.

3.1.2 Need For Names to be Meaningful

The common name of the Machine is a component of that DN, and is generated by the myGovID System in the application for the myGovID Machine Certificate. The name generated is meaningful, unambiguous and unique to the Certificate Holder.

Any disputes in relation to names in myGovID Machine Certificates will be resolved by the myGovID System Owner or delegate.

3.1.3 Anonymity or pseudonymity of Subscribers

Anonymity or pseudonymity is not supported

3.2 Initial Identity Validation

See section 3.2 of the CPS.

An Organisation Administrator nominates an individual to take on the role of the Machine Credential Administrator (MCA).

An application for a myGovID Machine Certificate must be made through the myGovID System by the MCA for the Organisation. The MCA supplies their full legal name and their Organisation issued email address

The MCA receives an email from Relationship Authorisation Manager (RAM)with their unique authorisation code which they will provide in RAM, and accept their authorisation. The MCA logs into RAM with their myGovID, places the Organisation for which they are now authorised into focus, selects the 'Machine credentials' tab and selects 'create machine credential'.

The MCA names their machine credential according to the naming convention stipulated in the CP. The MCA is recognised as the custodian of the machine credential the have created for their Organisation. The MCA accepts terms and conditions and downloads machine credential (downloads and runs browser extension if required).

The MCA downloads and stores the machine credential. The MCA notifies ATO of the credential serial number.

Please refer to Section 4.2, Section 4.3 and Section 4.5.1 of this CP.

3.2.1 Initial Machine Identity Validation

When applying for a myGovID Machine Certificate, the MCA initially identifies and authenticates themselves to the myGovID System using their myGovID User Certificate.

For the identity validation details required in order to obtain a myGovID User Certificate, see the myGovID Certificate Policy User section 3.2

In an application for a myGovID Machine Certificate (to be held for an Organisation), the MCA is selected from a list of individuals who hold a valid myGovID User Certificate for that same Organisation, and that MCA is initially identified and authenticated by reference to their Identity.

3.3 Identification and Authentication for Re-key Requests

myGovID Machine Certificates are re-keyed automatically.

The re-key process is described in sections 4.6 and 4.7 below.

3.3.1 Identification and Authentication for routine re-key

No stipulation

3.3.2 Identification and Authentication for re-key after revocation

See Section 3.2 of the CPS.

3.4 Identification and Authentication for Revocation Requests

If the revocation of a myGovID Machine Certificate is requested through the myGovID System by that Certificate Holder, that Certificate Holder identifies and authenticates themselves to the myGovID System using their myGovID (a website or application logon, including a valid password).

If a telephone request is made to a myGovID Operator for the revocation of a myGovID Machine Certificate (held by the Certificate Holder), the caller must provide sufficient identity details to allow the myGovID Operator, in accordance with existing ATO processes, to validate the caller's identity, and verify their status as that Certificate Holder.

All such revocation requests must come through the myGovID RA. The ATO CA will only action a revocation request if the ATO CA successfully validates the request by verifying the myGovID RA's signing certificate.

4 Certificate Life Cycle Operational Requirements

This section deals only with the life-cycle operational requirements for myGovID Machine Certificates. For life-cycle event details for myGovID User Certificates, see the applicable CP. Details of certain infrastructure certificates not used by any end entities may be found in the CPS. The certificate life-cycle events are described at a high-level, from the perspective of human end users.

Note: all certificate life-cycle event requests must come through a valid myGovID RA communication channel, using standards based formats such as Public Key Cryptography Standards (PKCS) payloads. At a technical level, a request will only succeed if the myGovID CA is able to successfully validate the request by verifying the myGovID RA's signing certificate.

4.1 Certificate Application

4.1.1 Who can submit an Application for a myGovID Machine Certificate?

An application for a myGovID Machine Certificate (to be held for an Organisation):

- > can only be made by the MCA for that same Organisation, and
- > can only be made online through the myGovID System, and
- > must hold a valid myGovID User Certificate as the custodian to be associated with that Machine Certificate.

4.2 Certificate Application Processing

For the purposes of this section an MCA is someone granted authority to issue machine credentials.

The process for an MCA for an Organisation applying for a myGovID Machine Certificate – to be held for that same Organisation – is generally as follows:

1. The MCA authenticates to the myGovID System using their myGovID User Certificate.
2. The MCA selects the new Machine option and follows the system prompts to:
 - enter the requested details of the Machine, including attributes identifying it (e.g. server name or IP address)
3. The MCA submits the application, which will begin the issuance process.
4. The MCA downloads the new machine credential and becomes the default custodian for the credential. Every credential created has a custodian (the MCA) who is responsible for the credential on behalf of the Organisation. The MCA is the logged on user, who is automatically registered as the custodian of the credentials they download.

4.3 Certificate Issuance

The typical issuance of a myGovID Machine Certificate includes these steps:

1. The myGovID System prompts the MCA to accept the *myGovID Machine Certificate Terms of Use*.
2. The MCA accepts those Terms of Use.
3. The MCA selects the location to which the myGovID Machine Certificate is to be downloaded and stored.
4. The system prompts the MCA to create and confirm a password to protect their Certificate, and the MCA enters and confirms the password.
5. The myGovID Machine Certificate is generated and downloaded to the selected file.
6. The myGovID System generates and stores a confirmation message that the myGovID Machine Certificate has been activated successfully.

4.4 Certificate Acceptance

The *myGovID Machine Certificate Terms of Use* set out responsibilities of the MCA of a myGovID Machine Certificate (and of the Organisation for which that Certificate is held) in relation to that Certificate. Responsibilities of the MCA are also set out in this CP. That MCA's acceptance of those Terms of Use constitutes acceptance of that Certificate. The use of that Certificate constitutes acceptance of:

1. that myGovID Machine Certificate, and
2. the *myGovID Machine Certificate Policy*, the *Certification Practice Statement*, and the *myGovID Machine Certificate Terms of Use* (in each case, as current as at the time of use).

4.4.1 Conduct constituting certificate acceptance

A certificate is deemed to have been accepted once it has been used.

4.4.2 Publication of the Certificate by the CA

See CPS Section 4.4.2

4.4.3 Notification of Certification Issuance by the CA to other entities

See CPS Section 4.4.3

4.5 Key Pair and Certificate Usage

myGovID Machine Certificates operate with a single Key Pair and have their key Usage extension set to include these values:

1. Digital Signature
2. Non-Repudiation

3. Key Encipherment
4. Data Encipherment.

This means that, for the purposes of both X.509 and this CP, a myGovID Machine Certificate may be used for (and its one Key Pair can be used for) both signing and encryption (confidentiality) purposes. However, encryption use should only be for traffic in transit. myGovID Machine Certificates are not designed to encrypt data long term, for example in a database.

Note: myGovID Relying Parties may only accept Machine Certificates for limited transactions and only then if their systems are designed to accept those transactions machine-to-machine.

Note: as the one key pair can be used for both Digital Signature and Data Encipherment, the private key must not be kept in escrow

4.5.1 Certificate Holder Responsibilities

The MCA for a myGovID Machine Certificate is responsible for:

- > downloading the Machine Certificate when it is issued, following registration
- > creating the password that protects the Machine Certificate and its associated Keys, and changing that password at recommended intervals
- > ensuring the Machine Certificate is attached to the correct Machine.
- > safely transferring the Machine Certificate from the download location to the server location, if required for example because the Organisation has an IT Outsourcing, SaaS or similar arrangement with another entity, and needs to transfer its Machine Certificate to that other entity's hosting location
- > managing the use of, and safeguarding, the Machine Certificate
- > requesting revocation of the Machine Certificate, when required.

Other responsibilities and obligations of the MCA are also set out in this CP, the myGovID Terms of use - Machine Certificate and the CPS.

Note: an Organisation remains responsible for any transactions performed on its behalf using its Machine Certificate, and for ensuring its Machine Certificate is managed in a secure manner. Before an Organisation enters onto an IT Outsourcing, SaaS or similar arrangement – particularly where its Machine Certificate is hosted by the 3rd party provider or the MCA is not its direct employee – it should obtain its own legal advice on managing those responsibilities under that arrangement.

4.5.2 Relying Party Responsibilities

Section 1.4 and 1.3.4 of this CP 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

Not supported

4.7 Certificate Re-Key

Certificate re-key is the process of generating a new Key Pair and issuing a new Certificate that certifies the new Public Key. The circumstances requiring certificate re-key are described in 4.7.1 of the CPS. All myGovID Machine Certificate re-keys occur as follows:

1. Whenever an existing myGovID Machine Certificate is used, the myGovID System checks the Certificate's expiration date.
2. If the myGovID Machine Certificate is due to expire within 14 months, the system initiates the re-key process (see section 4.5 above).
3. The new myGovID Machine Certificate is generated and downloaded to the local key store (where the existing myGovID is stored), silently, with no interaction with the MCA.
4. The next time the Machine attempts to authenticate using the existing myGovID Machine Certificate, the system selects the new myGovID Machine Certificate, confirms that it is functioning, and overwrites the old myGovID in the key store.
5. The system generates and stores a confirmation that the myGovID Machine Certificate has been re-keyed successfully. This confirmation is not displayed in the user interface.

The myGovID System has no limit on the number of re-key it will perform on a single Certificate.

If a myGovID Machine Certificate is not used within 14 months of its expiration date, it will expire at the end of its validity period (as set out in the Certificate Profile in section 7 below). The myGovID System will not re-key revoked or expired myGovID certificates. Instead, a new Certificate must be applied for and issued (see sections 3.2, 4.1 and 4.2 of this CP).

4.7.1 Who may Request Certification of a New Public Key

See 4.1.1 of this CP (Who can submit a certificate application).

4.7.2 Processing Certificate Re-Keying Requests

Processing of certificate re-key requests is consistent with the processing of new certificate requests. As detailed in 4.2 of this CP (Certificate Application Processing)

4.7.3 Notification of New Certificate Issuance to Subscribers

See 4.3 of this CP (Certificate Issuance)

4.7.4 Conduct Constituting Acceptance of a Re-Keyed Certificate

See 4.4.1 of this CP (Conduct constituting certificate acceptance)

4.7.5 Publication of the Re-Keyed Certificate by the CA

See CPS 4.4.2 (Publication of the certificate by the CA)

4.7.6 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificate modification is not supported by myGovID Machine Certificates.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

See CPS Section 4.9.1

4.9.2 Who may Request Revocation

Revocation of a myGovID Machine Certificate – held for an Organisation – may be requested by:

- > the MCA associated with that Certificate
- > an Administrator for or an Organisation Associate
- > the myGovID RA, or
- > the ATO.

Organisations cannot initiate revocation action when acting as Relying Parties.

4.9.3 Procedure for Revocation Request

The revocation of a myGovID Machine Certificate may be requested by the MCA associated with that Certificate, an Administrator for or an Organisation Associate identified in that Certificate, as follows:

- > The MCA authenticates to the myGovID System using their own myGovID User Certificate and requests the revocation of that myGovID Machine Certificate.
- > That MCA authenticates to the myGovID System using their own myGovID and requests the revocation of that myGovID Machine Certificate.
- > The MCA telephones a myGovID Operator, provides sufficient identity details to allow the myGovID Operator, in accordance with existing ATO processes, to validate their identity and their status as the MCA, and requests the revocation of that myGovID Machine Certificate.
- > That Administrator or an Organisation Associate telephones a myGovID Operator, provides sufficient identity details to allow the myGovID Operator, in accordance with existing ATO processes, to validate their identity and their status as an Administrator for

or an Organisation Associate, and requests the revocation of that myGovID Machine Certificate.

Access to revocation information will be through the published repositories. See CPS Section 2.1 and the certificates CRL Distribution Point for further information.

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 myGovID System Owner.

The myGovID 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 a CA Must Process the Revocation Request

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

4.9.6 Revocation Checking Requirement for Relying Parties

See CPS Section 4.9.6.

4.9.7 CRL Issuance Frequency

See CPS Section 4.9.7.

4.9.8 Maximum Latency for CRLs

See CPS Section 4.9.8.

4.9.9 On-line Revocation/Status Checking Availability

See CPS Section 4.9.9.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

See CPS Section 4.9.11.

4.9.12 Special Requirements re Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

See CPS Section 4.9.13.

4.9.14 Who Can Request Suspension

See CPS section 4.9.14.

4.10 Certificate Status Services

See CPS section 4.10.

4.11 End of Subscription

See CPS section 4.11.

4.12 Key Escrow and Recovery

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

See CPS section 4.12.

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 Archive

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

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 the 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 machine 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 CPS 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 myGovID 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 machine; 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

See CPS and Appendix A for further details

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: **{1.2.36.1.9001.1.1.8.1}**

7.1.7 Usage of Policy Constraints Extension

Policy constraints are not present.

7.1.8 Policy Qualifiers Syntax and Semantics

See Appendix A.

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 of Circumstances

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

Note: an order of precedence applies to the documents forming the applicable contract – see CPS section 1.1.4.

9.1 Fees

No stipulation.

9.2 Financial Responsibility

No stipulation.

9.3 Confidentiality of Business Information

See CPS Section 9.3.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The ATO PKI Privacy Notice conforms to the requirements of the *Privacy Act 1998 (Cth)* (*Privacy Act*) and Information Privacy Act 2014 (ACT). The myGovID Privacy Policy is available at <https://myGovID.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 1998 (Cth)). The collection, use and disclosure of such information is governed by the Privacy Act 1988 (Cth) and the Information Privacy Act 2014 (ACT).

9.4.2 Information Treated as Private

Personal information is not published in the digital Certificate and will be treated as private. Refer to the myGovID Privacy Policy for more information.

9.4.3 Information Not Deemed Private

See CPS Section 9.4.3.

9.4.4 Responsibility to Protect Private Information

See CPS Section 9.4.4.

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See CPS 9.4.6.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

See CPS Section 9.5.

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 Representation and Warranties

No stipulation.

9.6.4 Relying Parties Representation and Warranties

See CPS.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of all other Warranties

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.

See CPS section 9.7.

9.8 Limitation of Liability

See CPS section 9.8.

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 myGovID System Owner.

9.9 Indemnities

See CPS section 9.9.

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 section 9.11.

9.12 Amendments

See CPS section 9.12.

9.13 Dispute Resolution Procedures

See CPS section 9.13.

9.14 Governing Law

See CPS section 9.14.

9.15 Compliance with Applicable Law

See CPS section 9.15.

9.16 Miscellaneous Provisions

See CPS section 9.16.

Appendix A: Certificate Profiles and CRL Profiles and Formats

myGovID Machine 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 Machine associated with the private key. Common Name = <Device ID> O = <ABN> C = AU dnQualifier=<ABR>
subjectPublicKeyInfo	The public key and the public key algorithm (RSA 2048 with a SHA-256 digest).

Certificate Extensions	
Attribute	Value
Key size	2048

keyUsage	<p>Defines valid purposes, such as encipherment or signature, for the key contained in the certificate. Settings will include Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment. The values keyCertSign or crlSign are not allowed in Machine Certificates. See section 4.4 above for more information on valid usage of the single key pair.</p>
certificatePolicies	<p>CP information such as the OID and the URL where the CPS is available:</p> <p>[1]Certificate Policy: Policy Identifier=1.2.36.1.9001.1.1.8.1 [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.</p> <p>[2]Certificate Policy: [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://pki.ato.gov.au/policy/ca.html</p>
basicConstraints [critical]	<p>Indicates if the subject may act as a CA and should be set to "False"</p> <p>pathLengthConstraint=None</p>
cRLDistributionPoints	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://pki.ato.gov.au/crls/atosubca.crl</p>
extendedKeyUsage	<p>Defines additional valid purposes for the key contained in the certificate: clientAuthentication</p>
authorityInformationAccess	<p>[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.crl</p>

CRL Profile

CRL Attributes	
Attribute	Value
CRL issue period	90min
CRL validity	7 hours
CRL signature digest	SHA-256
revokedCertificates	List of revoked certificates by serial number.
reasonCode	Not used.
invalidityDate	Date at which it is known or suspected that the private key was compromised or that the certificate should otherwise be considered invalid.

