X.509 Certificate Policy
for the
New Zealand Government PKI
RSA Individual - Software Certificates
(Medium Assurance)

Version 1.0

Mar-21

Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy, identified by subarcs of the object identifier **2.16.554.101.8.1.2.3.1**, is only permitted as set forth in this document. Use of this document constitutes acceptance of the terms and conditions set out in this document. The acceptance of a certificate by a Relying Party for a prohibited purpose is at the Relying Party's risk. Engaging in a prohibited Certificate use is a breach of this Certificate Policy and the New Zealand Government disclaims any and all liability in such circumstances. The conditions applicable to each type of New Zealand Government Certificate will vary.

Document Management

This document is controlled by:	Cogito Group
Changes are authorised by:	Lead Agency

Change History

Version	Issue Date	Description/ Amendment	Changed by
0.1 Draft	Feb 2016	Initial draft	SJL
0.2	Mar 2016	Updates as per requirements from DIA	BF
0.3	Mar 2016	Review and minor updates, OIDs	SJL
0.4	Mar 2016	Review and minor updates	TB
0.5	Mar 2016	Update OIDs to include version extension	SJL
0.6	Apr 2016	Review and update minor typo errors	RB
0.7	Apr 2016	Update AIA/CDP/CP publication points	BB
0.8	Apr 2016	Update key length to 2048	BB
0.9	Apr 2016	Review and minor updates	BF
1.0	Aug 2020	Review and minor updates	BF

Signatures

Appointment	Organisation	Signature
Operations Manager	Cogito Group	
Lead Agency	DIA	

Contents

List of Tables

1. INTRODUCTION

Certificate policies are, in the *X.509* version 3 digital certificate standard, the named set of rules regarding the applicability of a *certificate* to a particular community (e.g. *the New Zealand Govt.*) and contain information about the specific structure of the relevant certificate type and grade.

This *Certificate Policy* (CP) identifies the rules to manage the New Zealand Govt. PKI Individual – Software (Medium Assurance) identity certificates, including the obligations of the *Public Key Infrastructure* (PKI) entities, and how the parties, indicated below, use them. It does not describe how to implement these rules as that information is in the *Certification Practice Statement* (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 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

This section identifies and introduces the set of provisions, and indicates the types of entities and *applications* applicable for this New Zealand Government PKI Individual – Software (Medium Assurance) Certificate (ID-MAC) Policy.

1.1 Overview

An ID-MAC is used to identify an individual who has an affiliation with the New Zealand Government (Staff, Subscriber Organisation, Contractor or Consultant etc.) and who has a requirement, which has been approved by the New Zealand Government, to:

i. Interact directly with New Zealand Government assets or systems, using *Public Key Technology* (PKT);
ii. Authenticate with a third party, as an affiliate of the New Zealand Government or customer organisation; or
iii. Provide a *digital signature*, as an individual *affiliated* with the New Zealand Government or subscriber organisation.

There are two types of certificates issued under this CP, namely:

i. Signing/authentication certificates; and
ii. Encryption/confidentiality certificates.

No authority, or privilege, applies to an individual by becoming an approved ID-MAC holder, other than confirming an affiliation with the organisation.

This CP allows *Subscribers*' *keys* and certificates to reside on soft or hardware based *tokens*.

1.2 Document name and identification

The title for this CP is "X.509 Certificate Policy for the New Zealand Govt. PKI Individual – Software (Medium Assurance) Certificates". The *Object Identifier* (OID) for this CP is 2.16.554.101.8.1.2.3.1

{ joint-iso-itu-t (2) member-body (16) NZ (554) Govt (101) pki (8) certificate policy (1) individual (2) Software (3) Version (1)}

1.3 PKI participants

1.3.1 Certification authorities

The *Certification Authority* (CA), or CAs, that issue certificates under this CP are New Zealand Government CAs.

1.3.2 Registration authorities

The *Registration Authority* (RA), or RAs, that perform the registration functions under this CP are authorised by the Lead Agency. For those certificates issued in accordance with the accreditation, an accredited RA must be used. An RA is formally bound to perform the registration functions in accordance with this CP and other relevant *Approved Documents*.

1.3.3 Subscribers

A *Subscriber* is defined in Appendix B of the CPS to be, as the context allows:

a) the entity (e.g. an individual, device, web site, application or resource) whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant Certificate, and / or
b) the person or legal entity that applied for that Certificate, and / or entered into the Subscriber Agreement in respect of that Certificate.

Without limiting the foregoing, in this CP the Subscriber generally refers to the individual whose name appears as the subject in a certificate. Subscribers in this context include any individual that has been approved as having a requirement to be authenticated as affiliated with the New Zealand Government. Subscribers in this context include:

i. New Zealand Government personnel;
ii. Subscriber Organisations personnel;
iii. Contractors, Consultants and Professional Service Providers (individuals); and
iv. Other individuals approved by the New Zealand Government as having a requirement for an ID-MAC.

A Subscriber issued a certificate under this CP does not automatically receive access, authority or privilege to New Zealand Government assets or systems. New Zealand Government assets and systems may act as a *Relying Party* having granted access, authority or privilege to an individual.

1.3.4 Relying parties

A Relying Party uses an ID-MAC to:

i. Verify the identity of a Subscriber;
ii. Verify the integrity of a communication with the Subscriber;
iii. Establish confidential communications with a Subscriber; and
iv. Ensure the non-repudiation of a communication with a Subscriber.

Before relying on the Subscriber certificate, a Relying Party must:

i. verify the validity of a digital certificate;
ii. verify that the digital certificate is being used within the limits specified in the CP; and
iii. promptly notify the RA in the event that it suspects that there has been a compromise of the Subscriber's *Private Keys*.

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

i. The processes of checking validity of the Subscriber's certificate;
ii. Any authority, or privilege, of the Subscriber to act on behalf of the New Zealand Government; and

iii. Any authority, access or privilege the Subscriber has to the Relying Party's assets or systems.

A Relying Party agrees to the conditions of this CP and the CPS. The use of a certificate, or associated revocation information, issued under this CP is the Relying Party's acceptance of the terms and conditions of this CP and CPS.

1.3.5 Other participants

Other participants include:

i. The *Lead Agency* – refer to the CPS for their responsibilities which specifically include:

   a) Review and approval of this CP;
   b) Presiding over the PKI audit process;
   c) Approving mechanisms and controls for the management of the accredited infrastructure (CA/RA); and
   d) Approval of operational standards and guidelines to be followed.

ii. *Accreditation Agencies* – to provide independent assurance that the facilities, practices and procedures used to issue ID-MACs comply with this CP, the Certification Practice Statement and other relevant documentation (policy and legal).

iii. *Directory Service* providers – to provide a *repository* for certificates and certificate status information issued under this CP.

1.4 Certificate usage

Certificates issued under this CP, in conjunction with their associated private keys, allow a Subscriber to:

i. Authenticate themselves to a Relying Party electronically in online transactions;
ii. Digitally sign electronic documents, transactions and communications; and
iii. Confidentially communicate with a Relying Party.

1.4.1 Appropriate certificate uses

Certificates issued under this CP, in conjunction with their associated private key, may be used:

i. For the authentication of the identity of a Subscriber, during the conduct of any lawful business with that individual, as an individual affiliated with the New Zealand Government and for which the *level of assurance* has been assessed as sufficient by the Lead Agency and the Relying Party organisation;
ii. To provide accountability and non-repudiation of ID-MAC Subscriber transactions or communications;
iii. To verify the integrity of a communication from a Subscriber to a Relying Party; and
iv. For the sending and receiving of confidential communications, provided such communication is in accordance with normal New Zealand Government business and security policy and procedures.

Relying Parties should note the risks identified as per Appendix D in relation to the New Zealand Government requirements of Individual - Software (Medium Assurance) RSA certificates.

1.4.2 Prohibited certificate uses

The prohibited uses for certificates issued under this CP are:

i. To use the certificate in a way that represents that the certificate possesses any attribute, authority, access, privilege or delegations that may be afforded to the Subscriber.

ii. To use the certificate in a way that represents that communications and transactions can only occur over certain specified infrastructure for that transaction or communication.
iii. For a Subscriber to conduct any transaction, or communication, which is any or all of the following:

a) Unrelated to organisational business;
b) Illegal;
c) Unauthorised;
d) Unethical, or
e) Contrary to New Zealand Government policy.

The acceptance of a certificate by a Relying Party for a prohibited purpose is at the Relying Party's risk. Engaging in a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the Subscriber and the New Zealand Government disclaims any and all liability in such circumstances.

1.5 Policy administration

1.5.1 Organisation administering the document

See CPS.

1.5.2 Contact person

See CPS.

1.5.3 Authority determining CPS suitability for the policy

See CPS.

1.5.4 CPS approval procedures

See CPS.

1.6 Definitions, acronyms and interpretation

Acronyms and terms used in this CP are defined in the CPS. Note that 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 CP. Defined terms may be upper or lower case.

The interpretation clause in Part 3 of Appendix B of the CPS (B.3) also applies to this CP.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See CPS.

2.2 Publication of certificate information

The New Zealand Government 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 New Zealand Government.

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

i. This CP; and
ii. The CPS.

2.3 Time or frequency of publication

Published documentation is updated on approved change.

The issuing CA publishes new certificates and CRL at least once every 10 days.

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:

i. Must have a clear distinguishable and unique *Distinguished Name* (DN) in the certificate subjectName field;
ii. Will have as an alternative name in the subjectAltName field the Subscriber's organisation email address, as well as the Microsoft Unique Principal Name (UPN); and
iii. Must have common name components of the name, for both the subjectName and subjectAltName that are unique to the individual within the organisation name space.

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

To achieve a unique DN the Common Name (CN) component is based on the Subscriber's organisation email address.

3.1.2 Need for names to be meaningful

Names used to identify the Subscriber are to be based on the Subscriber's organisation email address and:

i. Relate to identity of the Subscriber as provided by the *Directory* entry;
ii. Must not identify the Subscriber by role or position; and
iii. *Evidence of Identity* (EOI) information verifying the identity of the Subscriber must relate to the Subscriber's Directory entry.

3.1.3 Anonymity or pseudonymity of Subscribers

This CP prohibits using an anonymous or pseudonymous Subscriber name.

However, the Subscribers common name as identified in the Directory may be used if it is their organisation email address as well.

3.1.4 Rules for interpreting various name forms

No stipulation as there is only one form.

3.1.5 Uniqueness of names

Names are unique within the organisation name space. Names used in certificates are unique to the individual and valid for that individual irrespective of their affiliation or relative location to, or within the organisation.

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 creation of a network account initiates the certificate issuance.

A soft token containing the *key pair* is generated for the individual on the workstation the first time the user logs in to their account. To prove possession of the private key, a digitally-signed certificate request is submitted to the RA. The submission is made using the credentials supporting access to the individuals account within the *Information Environment* (IE).

3.2.2 Authentication of organisation identity

To be identified as *affiliated* with the New Zealand Government or a subscribing organisation the Subscriber must be identified by their organisation.

3.2.3 Authentication of individual identity

Prior to certificate issuance the individual's identity is authenticated by the following processes:

i. The Subscriber undergoes the organisations process to obtain access to the organisations network. This process validates the Subscriber's identity.
ii. The Subscriber's identity is re-validated as part of the process to issue a facility access card (positive face-to-face identification using a government issued token with photograph).
iii. Depending on the Subscriber's role within the organisation, the Subscriber is:
    a) Registered within the *Personnel Management* system for that organisations employees; or
    b) Registered within the organisations system for contractors.
iv. To obtain a network account, the Subscriber's sponsor validates the Subscriber's security clearance (if applicable), positively identifies the applicant (Drivers Licence, Passport, etc), confirms the Directory entry and submits a network access request.

The Directory is used as the authoritative source when creating a user's account within the organisation.

3.2.4 Non-verified subscriber information

All Subscriber information contained in a certificate is verified by the subscriber organisation.

3.2.5 Validation of authority

Applicants must have an account within the subscriber organisation IE, thus the affiliation with the organisation is validated.

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*. Authentication to the network automatically generates a routine re-key, where applicable.

3.3.2 Identification and authentication for re-key after revocation

See 3.2 (Initial Identity Validation).

3.4 Identification and Authentication for Revocation Requests

Certificates issued through auto-enrolment are normally not revoked; if there is a need to revoke because of actual or suspected compromise, the account will be disabled or disconnected. If a Subscriber knows or suspects that their Windows login has been compromised, they must contact network support immediately. Identification for such a support call follows normal organisation procedures.

See 4.9 (Certificate revocation and suspension) 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 an approved affiliation with the New Zealand Government or subscriber organisation, and who has been assigned a user account in a subscriber organisation IE is eligible for an ID-MAC.

4.1.2 Enrolment process and responsibilities

Once the process described in 3.2.3 (Authentication of individual identity) has been completed and an applicant has been granted a network user account, the act of the applicant logging on for the first time initiates the certificate application process. This process is automated, using Windows' auto-enrol feature integrated with the New Zealand Government PKI.

The applicant's supervisor (or sponsor) is responsible for submitting the request for a network account via organisation system procedures. The supervisor or sponsor must validate the applicant's identity against their record in the Directory and ensure their security clearance is sufficient for the network account requested.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

See 3.2.3 (Authentication of individual identity)

4.2.2 Approval or rejection of certificate applications

All requests that meet the conditions of the policy permissions 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 New Zealand Government PKI 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 auto-enrolment process returns the certificate directly to the Subscriber's certificate store within the specific network that the Subscriber is connected to. 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.

4.4.2 Publication of the certificate by the CA

The New Zealand Government PKI repository will publish certificates as required. Applicable certificates will be available in external New Zealand Government repositories.

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 1.4 (Certificate Usage). Subscriber responsibilities are described below in 9.6.3 (Subscriber Representations and Warranties).

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

1.4 (Certificate Usage) and 1.3.4 (Relying Parties) detail the Relying Party's *public key* and certificate usage and responsibilities.

The interpretation and compliance with extended KeyUsage attributes, and any associated limitations on the use of the certificate and/or private key, is in accordance with RFC6818.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

This CP permits certificate renewal. The criteria for certificate *renewal* are defined in the CPS.

4.6.2 Who may request renewal

See 4.1.1 (Who can submit a certificate application).

4.6.3 Processing certificate renewal requests

The process for certificate renewal is consistent with the enrolment process defined in 4.1 (Certificate Application). The identification and authentication procedures must comply with 3.3 (Identification and Authentication for Re-Key Requests).

4.6.4 Notification of new certificate issuance to subscriber

See 4.3.2 (Notification to subscriber by the CA of issuance of certificate).

4.6.5 Conduct constituting acceptance of a renewal certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.6.6 Publication of the renewal certificate by the CA

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

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 CP permits certificate re-key. See CPS for relevant circumstances.

4.7.2 Who may request certification of a new public key

Certificate re-key may be requested by the:

i. Lead Agency; or
ii. Subscriber.

4.7.3 Processing certificate re-keying requests

The process for certificate re-key is consistent with the enrolment process defined in 4.1 (Certificate Application). The identification and authentication procedures must comply with 3.3 (Identification and Authentication for Re-Key Requests).

4.7.4 Notification of new certificate issuance to subscriber

See 4.3.2 (Notification to subscriber by the CA of issuance of certificate).

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.7.6 Publication of the re-keyed certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

This CP does not support *certificate modification*. If a certificate needs to be modified, it will be re-keyed.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

If a Subscriber's account has been compromised, or the identification of the Subscriber changes, they are obliged to report this to the relevant IE support channel. The account itself will then be disabled or re-keyed, requiring the Subscriber to create a new password. Its Auto-enrol Certificate will not normally be revoked or suspended.

An Auto-enrol Resource Certificate may be revoked where an authorised revocation requestor (see CPS 4.9.2) consider it desirable to do so.

4.9.2 Who can request revocation

See CPS.

4.9.3 Procedure for revocation request

Where used, revocation requests received by *Authentication Services (AS) Operators* are to be verified on receipt in accordance with 3.4 (Identification and authentication for revocation request) and processed in priority order.

After verification the *Registration Officer (RO)* or AS Operator processes revocation requests by 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.

4.9.4 Revocation request grace period

A grace period of one *Operational Day* is permitted.

The Lead Agency, 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.

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 Party's responsibility to determine their requirement for revocation checking.

Certificates issued under this CP are unsuitable for a Relying Party's use if the requirements for revocation checking conflict with the clauses in 4.9 of this CP.

4.9.7 CRL issuance frequency (if applicable)

Refer to the issuing CA's CP for CRL issuance frequency

4.9.8 Maximum latency for CRLs (if applicable)

Refer to the issuing CA's CP.

4.9.9 On-line revocation/status checking availability

Online Certificate Status Protocol service (OCSP) is available at:

http://ocsp.pki.govt.nz/

Refer to the relevant Certificate Profile in Appendix B - if the certificate is issued with an OCSP access location reference (Authority Information Access extension), OCSP is available to the Relying Party as a certificate status checking method.

The latest CRL is available from the published repositories; refer to 2.1 (Repositories) 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.

Externally the New Zealand Government will provide the required certificates and the most up-to-date CRL.

4.10.1 Operational characteristics

See CPS.

4.10.2 Service availability

See CPS.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

See CPS.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Escrow practices differ for the two types of private keys issued under this CP (see 1.1)

Escrow, backup and archiving of private authentication keys issued is not permitted under this CP. However, escrow and backup of *private confidentiality keys* is permitted.

The *Authorised Key Retriever* (AKR) must submit either a signed email or memorandum to an RO or AS operator. The operator undertakes recovery of a private confidentiality key from escrow after validating the identity of the AKR and rationale for the recovery. After validation, the RO uses the approved software to implement the process, which will log the transaction.

4.12.2 Session key encapsulation and recovery policy and practices

Symmetric keys are not required to be escrowed.

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 in the operating system's cryptographic application programming interface (API) during the requesting process based on rules defined by the account creation policy.

6.1.2 Private key delivery to subscriber

The key generation is performed on the Subscriber's workstation and stored directly in the Subscriber's operating system certificate store, so no delivery is required.

Private confidentiality keys, if issued, are always encrypted in transit.

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

See Appendix B.

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 1.4 (Certificate Usage).

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 New Zealand Government PKI.

Key usages are specified in the Certificate Profile set forth in Appendix B.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

Subscriber keys are stored in the user account certificate store, protected by the Subscriber's user account password.

HSMs used with the PKI core components are on the Evaluated Products List (EPL).

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

See CPS.

6.2.3 Private key escrow

Escrow of private authentication keys does not occur; however, private confidentiality keys are subject to escrow. Refer to CPS for escrow controls.

6.2.4 Private key backup

See CPS.

6.2.5 Private key archival

See CPS.

6.2.6 Private key transfer into or from a cryptographic module

See CPS.

Private confidentiality keys, if issued, are escrowed, and will be stored in encrypted form in the key management archive. Private confidentiality keys are always transferred using the *PKI software* confidentiality key(s).

6.2.7 Private key storage on cryptographic module

See CPS.

6.2.8 Method of activating private key

To activate key usage, the Subscriber must authenticate into their organisation IE account, which gives the Subscriber access to the token associated with the Subscriber's key pair.

6.2.9 Method of deactivating private key

The Subscriber's private key will be deactivated when they log out of the network account to which the certificate has been issued.

6.2.10 Method of destroying private key

See CPS.

6.2.11 Cryptographic Module Rating

See 6.2.1 of this CP.

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 shall be kept in accordance with New Zealand Govt. security policy.

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

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

i. Identity Signature/Authentication Certificate; and
ii. Identity Encryption/Confidentiality Certificate.

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 B.

7.1.3 Algorithm object identifiers

Certificates under this CP will use one of 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 certify only public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign certificates, CRL*s* and any other PKI product, including other forms of revocation information, such as OCSP responses.

7.1.4 Name forms

The Common Name (CN) component is based, where possible, on the Subscriber's organisation's email address and/or be unique in the subscriber organisation. It is encoded as an X.501 printable string where possible, and using UTF-8 otherwise.

All other DN components are fixed and defined in Appendix B.

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:

{2.16.554.101.8.1.2.3.1}

Certificates issued under this policy shall also assert the following LoA OID:

{2.16.554.101.8.2.1.2.1} Level of Assurance – Medium (Individual)

In addition; to enable the use of the certificate at lower Levels of Assurance, this policy also asserts the following OID:

{2.16.554.101.8.2.1.1.1} Level of Assurance – Low (Individual)

See also Appendix B.

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 C.

7.3 OCSP profile

7.3.1 Version Numbers

OSCP is implemented using version 1 as specified under RFC6960.

7.3.2 OCSP Extensions

Refer to CPS and Validation Authority (VA) CP for full OCSP profile.

8. COMPLIANCE AUDIT 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 regarding fees for access to this CP. No fee has been stipulated for other services.

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, any authority, access or privilege. Relying Parties assume responsibility for any financial limit they may wish to apply for transactions authenticated using certificates issued under this CP.

9.2.1 Insurance

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

In order to provide an audit and evidentiary trail of the verification process, and documentation presented to confirm an individual's identity, The New Zealand Government is required to collect Personal Information (as defined in the *Privacy Act 1993*). The collection, use and disclosure of such information is governed by the Privacy Act 1993 (Privacy Act).

At enrolment, applicants acknowledge that the New Zealand Government may collect, use or disclose Personal Information about them, for the purposes discussed below.

The New Zealand Government PKI Privacy Statement is available from http://www.pki.govt.nz/policy/.

9.4.2 Information treated as private

Personal Information, other than the name and e-mail address of the applicant, is not published in the Digital Certificate. The New Zealand Government PKI relies on the Subscriber being given an account within the subscriber organisation's network, and relies on the management of Evidence of Identity (EOI) documentation presented and the unique document identifiers.

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

Consent by the Subscriber to the use of Personal Information is given by signing the organisations network request.

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

The Subscriber, in obtaining access to the network warrants that the information provided by them is true to the best of their knowledge. In addition, Subscribers warrant to:

i. only use Keys and digital certificates within the limits specified in the CP;
ii. take all reasonable measures to protect their Private Key(s) from compromise and take all necessary precautions to prevent loss, disclosure, modification, or unauthorised use of their Private Key(s);
iii. promptly notify the RA in the event that they consider or suspect there has been a compromise of their Private Key(s); and
iv. promptly notify the RA in the event that they consider the EOI information provided by them is or may be incorrect.

9.6.4 Relying party representations and warranties

See CPS.

9.6.5 Representations and warranties of other participants

No Stipulation.

9.7 Disclaimer of warranties

See CPS.

9.8 Limitations of liability

See CPS.

In addition, the Lead Agency is only responsible for performing the accreditation process with due care, in adherence to published New Zealand Government Criteria and Policies. The New Zealand Government is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the Lead Agency.

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 shall remain in effect until the notice of its termination is communicated by the New Zealand Government 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:

i. Laws; and
ii. New Zealand Government Policies.

9.16 Miscellaneous provisions

See CPS.

9.17 Other provisions

See CPS.

APPENDIX A. REFERENCES

The following documents are referenced in this CP:

[CPS]	X.509 Certification Practice Statement for the New Zealand Government PKI, available at http://www.pki.govt.nz/policy/
[6960]	RFC6960 Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol (OCSP), Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc6960.txt
[3647]	RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc3647.txt
[6818]	RFC6818 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc5280.txt
[KMP]	The New Zealand Government Authentication Services Key Management Plan
[RCA CP]	X.509 Certificate Policy for the NZ Government Root Certification Authority and Subordinate Certificate Authorities, available at http://www.pki.govt.nz/policy
[VA CP]	X.509 Certificate Policy for New Zealand Government Validation Authority Certificates, available at http://www.pki.govt.nz/policy
[Privacy Act]	New Zealand Privacy Act 1993 http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

Table 3 - References

APPENDIX B. CERTIFICATE PROFILES

NB. Variations to the Certificate Profiles associated with this Annex will occur over time due to technical implementations. As such variations will be marginal and not materially affect the certificates issued under this CP. They will not be reviewed by the Gatekeeper Competent Authority.

B.1 Individual – Software (Medium Assurance) Certificate - Authentication

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		Randomly Generated Number	Unique value generated by the issuing CA
Issuer signature algorithm		SHA256WithRSAEncryption	
Issuer distinguished name		CN= NZGovtCA<serial> OU= CAs OU= PKI O= Govt C= NZ	<Serial> denotes the number after "NZGovtCA" that represents the issuing CA and is expected to start at "301".
Validity period		Not before <UTCtime> Not after <UTCtime>	2 years from date of issue
Subject distinguished name		CN=<LHS of Agency email alias> OU=<Agency> OU=PKI O=Govt C=NZ	Note: Example only, actual naming will reflect the subscriber organisation. CN must be unique within the subscribing organisations namespace An example would be the use of the left hand side of the Subject's organisational email address, e.g. "Rob.Smith7" for a subject with the principal email address "rob.smith7@dia.govt.nz" Encoded as printable string where possible, and otherwise using UTF-8
Subject public key information		2048 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
X.509 V3 extensions:			
Authority key identifier	No	<octet string>	256 bit SHA256 hash of binary DER encoding of signing CA's public key
Subject key identifier	No	<octet string>	256 bit SHA256 hash of binary DER encoding of subject's public key
Key usage	No	digitalSignature nonrepudiation	
Extended key usage	No	{1.3.6.1.5.5.7.3.2} Microsoft Client Authentication {1.3.6.1.5.5.7.3.4} Secure email protection	

Field	Critical	Value	Notes
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy ID:{**2.16.554.101.8.1.2.3.1**} Policy Qualifier: Policy Qualifier – User Notice: explicitText, <"Other than confirming affiliation with the New Zealand Govt, the New Zealand Govt PKI infers no authority or privilege to the Subscriber of this certificate. Certificates must not be used for any purpose not permitted by the Certificate Policy" CPS Pointer: https://www.pki.govt.nz/policy/	The OID of CP.
		[2] Policy OID: {**2.16.554.101.8.2.1.2.1**}	Level of Assurance – Medium The Level of Assurance of this certificate
		[3] Policy OID: {**2.16.554.101.8.2.1.1.1**}	Level of Assurance – Low Included to allow the certificate to be used in lower assurance context.
Policy mapping		-	Not Present
Subject Alternative Name		RFC822 Name (email address) Other Name: Principal Name	
Issuer alternative name		-	Not Present
Subject directory attributes		-	Not Present
Basic constraints		-	Not Present
Name constraints		-	Not Present
Policy constraints		-	Not Present
Authority Information Access	No	[1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt [2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c [3] Access method=OCSP {1.3.6.1.5.5.7.48.1}: Access location: http://ocsp.pki.govt.nz/	
CRL Distribution Point	No	[1] Distribution Point Name (http): http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl [2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).
Microsoft Certificate Template		User Authentication	

Table 4 – Certificate Profile User Authentication

B.2 Individual – Software (Medium Assurance) Certificate - Confidentiality

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		Randomly Generated Number	Unique value generated by the issuing CA
Issuer signature algorithm		SHA256WithRSAEncryption	
Issuer distinguished name		CN= NZGovtCA<serial> OU= CAs OU= PKI O= Govt C= NZ	<Serial> denotes the number after "NZGovtCA" that represents the issuing CA and is expected to start at "301".
Validity period		Not before <UTCtime> Not after <UTCtime>	2 years from date of issue
Subject distinguished name		CN=<LHS of organisation email alias> OU=Personnel OU=PKI O=Govt C=NZ	Note: Example only, actual naming will reflect the subscriber organisation. CN must be unique within the subscribing organisations namespace An example would be the use of the left hand side of the Subject's organisational email address, e.g. "Rob.Smith7" for a subject with the principal email address "rob.smith7@dia.govt.nz" Encoded as printable string where possible, and otherwise using UTF-8
Subject public key information		2048 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
X.509 V3 extensions:			
Authority key identifier	No	<octet string>	256 bit SHA256 hash of binary DER encoding of signing CA's public key
Subject key identifier	No	<octet string>	256 bit SHA256 hash of binary DER encoding of subject's public key
Key usage	No	keyEncipherment dataEncipherment	
Extended key usage	No	{1.3.6.1.5.5.7.3.4} Secure email protection	
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy ID:**{ 2.16.554.101.8.1.2.3.1**} Policy Qualifier: CPS Pointer: https://www.pki.govt.nz/policy/	This CP
		[2] Policy OID: {**2.16.554.101.8.2.1.2.1**}	Level of Assurance – Medium The Level of Assurance of this certificate

Field	Critical	Value	Notes
		[3] Policy OID: {**2.16.554.101.8.2.1.1.1**}	Level of Assurance – Low Included to allow the certificate to be used in lower assurance context.
Policy mapping		-	Not Present
Subject Alternative Name		RFC822 Name (email address) Other Name: Principal Name	
Issuer alternative name		-	Not Present
Subject directory attributes		-	Not Present
Basic constraints		-	Not Present
Name constraints		-	Not Present
Policy constraints		-	Not Present
Authority Information Access	No	1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt [2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c [3] Access method=OCSP {1.3.6.1.5.5.7.48.1}: Access location: http://ocsp.pki.govt.nz	
CRL Distribution Point	No	[1] Distribution Point Name (http): http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl [2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).
Microsoft Certificate Template		User Encryption	

Table 5 – Certificate Profile User Confidentiality

APPENDIX C. CRL FORMAT

Please refer to the issuing CA's Certificate Policy.

APPENDIX D. Level of Assurance Mapping

Assurance Level

The following table documents the mapping of this CP to the requirements of an associated assurance level as documented in the New Zealand Govt. PKI Assurance Level Requirements paper [LOA]:

CP's Level of Assurance:	Medium Assurance {**2.16.554.101.8.2.1.2.1**}. **As documented in section 7.1.6 above.**

REQUIREMENT	CP'S MAPPING TO REQUIREMENT
IDENTITY PROOFING	
EOI	The Subscriber must have an account on an affiliated organisations network, as well as have a current Security Clearance, where the subscriber must prove their identity, as covered in section 3.2 above.
Evidence of Relationship	Subscriber must be identified in the organisations directory, as covered in section 3.2.3 above.
Location	As documented in section 3.2.3, a Subscriber must have their Security Clearance validated, and then present locally to receive their organisations facility access card into a organisations site, and if authorised, will additionally be given access to the organisations network, this can occur locally or remotely, through the use of a split initial passphrase. Once authenticated into a network, the operating system will automatically provide the Subscriber with their soft token stored within the operating system certificate store.
CREDENTIAL STRENGTH	
Token Protection	As documented in section 6.2, the soft token supported by this CP is stored within the Subscriber's certificate store within the network where the account resides. Access to the certificate store is protected by access to the Subscriber's account within the network, which is password protected in alignment with the security requirements.
Token Activation	As documented in section 6.2.8, access to the token is activated on authentication to the Subscriber's account within the relevant network.
Life (Time) of Key Strength	As documented in Appendix B, the Key Strength will be RSA 2048 and SHA256 which in accordance with NIST SP800-57-1.
CERTIFICATE MANAGEMENT	
CA Protection	The CA is both physically and logically secure from the unauthorised access. The CA protection requirements are documented in the CPS and sections 5 and 6 of this CP.

Binding	As documented in section 4, the issuance of the ID-MAC through the Microsoft Windows auto enrol process binds the certificate issuance to the Subscriber's access to their organisation's network account. While the issuance process is not necessarily contiguous, the identity of the Subscriber is bound to their organisation email address.
Revocation (Publication)	As covered in section 4.9.7, the CRL is published weekly, or on a certificate revocation, which exceeds the requirements. This is as a result of issuing from the High Assurance CA.
Compliance	The Compliance requirements are covered in the CPS and section 8 (Compliance audit and other assessments). The New Zealand Government PKI environment is certified under the New Zealand Government accreditation program, to support the issuance of up to a High Assurance level.

A.1 Risk Assessment

The issuances of certificates using the ID-MAC Certificate Policy has been aligned with New Zealand Govt. Medium Assurance.

Any deviations within the CP from those requirements documented for the associated assurance level should be appropriately risk managed.

The following risks were identified and managed in the alignment of the ID-MAC with the requirements for Medium Assurance. The Lead Agency has accepted the risks through the appropriateness of the controls listed.

LOA REQUIREMENT	IDENTIFIED RISK	MITIGATION / CONTROLS
Token Protection	There is a risk that the soft token can be used by other parties. (The soft token containing the Subscriber's key pair is stored within the operating system's certificate store within the Subscriber's network account.)	• The New Zealand Govt. agency network administrators must have a security clearance to at least the level of the network, and they are educated on their responsibilities with regard to need-to-know. • The New Zealand Govt. agency has auditing of administration access. • Access to a Subscribers network account is protected with a passphrase, which meets the complexity requirements.
Token Activation	There is a risk that the soft token can be used by other parties. (The soft token containing the Subscriber's key pair doesn't require authentication for direct activation.)	• The soft token is stored within the Subscriber's operating system certificate store. • Access to a Subscribers network account is protected with a passphrase, which meets the complexity requirements. • As per the network security requirements, the Subscriber is required to 'lock' their workstation if they leave it