Cogito Group

DIGITAL IDENTITY AND SECURITY

X.509 Certificate Policy for the New Zealand Government PKI RSA Individual - Hardware Certificates (High 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 **2.16.554.101.8.1.2.4.1**, 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 PKI 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 with 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

1. INTRODUCTION 8
1.1 Overview 8
1.2 Document name and identification 9
1.3 PKI Participants 9
1.3.1 Certification authorities 9
1.3.2 Registration authorities 9
1.3.3 Subscribers 9
1.3.4 Relying Parties 9
1.3.5 Other participants 10
1.4 Certificate usage 10
1.4.1 Appropriate certificate uses 10
1.4.2 Prohibited certificate uses 11
1.5 Policy administration 11
1.5.1 Organisation administering the document 11
1.5.2 Contact person 11
1.5.3 Authority determining CPS suitability for the policy 11
1.5.4 CPS approval procedures 11
1.6 Definitions, acronyms and interpretation 11
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 11
2.1 Repositories 11
2.2 Publication of certification information 12
2.3 Time or frequency of publication 12
2.4 Access controls on repositories 12
3. IDENTIFICATION AND AUTHENTICATION 12
3.1 Naming 12
3.1.1 Types of names 12
3.1.2 Need for names to be meaningful 12
3.1.3 Anonymity or pseudonymity of Subscribers 12
3.1.4 Rules for interpreting various name forms 13
3.1.5 Uniqueness of names 13
3.1.6 Recognition, authentication, and role of trademarks 13
3.2 Initial identity validation 13
3.2.1 Method to prove possession of private key 13
3.2.2 Authentication of organisation identity 13
3.2.3 Authentication of individual identity 13
3.2.4 Non-verified Subscriber information 14
3.2.5 Validation of authority 14
3.2.6 Criteria for interoperation 14
3.3 Identification and authentication for re-key requests 14
3.3.1 Identification and authentication for routine re-key 14
3.3.2 Identification and authentication for re-key after revocation 14
3.4 Identification and authentication for revocation request 15
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 15
4.1 Certificate application 15
4.1.1 Who can submit a certificate application 15
4.1.2 Enrolment process and responsibilities 15
4.2 Certificate application processing 16

4.2.1 Performing identification and authentication functions 16
4.2.2 Approval or rejection of certificate applications 16
4.2.3 Time to process certificate applications 16
4.3 Certificate issuance 16
4.3.1 CA actions during certificate issuance 16
4.3.2 Notification to Subscriber by the CA of issuance of certificate 17
4.4 Certificate acceptance 17
4.4.1 Conduct constituting certificate acceptance 17
4.4.2 Publication of the certificate by the CA 17
4.4.3 Notification of certificate issuance by the CA to other entities 17
4.5 Key pair and certificate usage 17
4.5.1 Subscriber private key and certificate usage 17
4.5.2 Relying Party public key and certificate usage 17
4.6 Certificate renewal 17
4.6.1 Circumstance for certificate renewal 17
4.6.2 Who may request renewal 17
4.6.3 Processing certificate renewal requests 17
4.6.4 Notification of new certificate issuance to Subscriber 17
4.6.5 Conduct constituting acceptance of a renewal certificate 18
4.6.6 Publication of the renewal certificate by the CA 18
4.6.7 Notification of certificate issuance by the CA to other entities 18
4.7 Certificate re-key 18
4.7.1 Circumstance for certificate re-key 18
4.7.2 Who may request certification of a new public key 18
4.7.3 Processing certificate re-keying requests 18
4.7.4 Notification of new certificate issuance to Subscriber 18
4.7.5 Conduct constituting acceptance of a re-keyed certificate 18
4.7.6 Publication of the re-keyed certificate by the CA 18
4.7.7 Notification of certificate issuance by the CA to other entities 18
4.8 Certificate modification 18
4.8.1 Circumstance for certificate modification 18
4.8.2 Who may request certificate modification 19
4.8.3 Processing certificate modification requests 19
4.8.4 Notification of new certificate issuance to Subscriber 19
4.8.5 Conduct constituting acceptance of modified certificate 19
4.8.6 Publication of the modified certificate by the CA 19
4.8.7 Notification of certificate issuance by the CA to other entities 19
4.9 Certificate revocation and suspension 19
4.9.1 Circumstances for revocation 19
4.9.2 Who can request revocation 19
4.9.3 Procedure for revocation request 19
4.9.4 Revocation request grace period 20
4.9.5 Time within which CA must process the revocation request 20
4.9.6 Revocation checking requirement for Relying Parties 20
4.9.7 CRL issuance frequency (if applicable) 20
4.9.8 Maximum latency for CRLs (if applicable) 20
4.9.9 On-line revocation/status checking availability 20
4.9.10 On-line revocation checking requirements 20
4.9.11 Other forms of revocation advertisements available 20
4.9.12 Special requirements re key compromise 20

4.9.13 Circumstances for suspension 20
4.9.14 Who can request suspension 20
4.9.15 Procedure for suspension request 20
4.9.16 Limits on suspension period 21
4.10 Certificate status services 21
4.11 End of subscription 21
4.12 Key escrow and recovery 21
4.12.1 Key escrow and recovery policy and practices 21
4.12.2 Session key encapsulation and recovery policy and practices 21
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 21
5.1 Physical controls 21
5.2 Procedural controls 21
5.3 Personnel controls 21
5.4 Audit logging procedures 21
5.5 Records archival 21
5.6 Key changeover 22
5.7 Compromise and disaster recovery 22
5.8 CA or RA Termination 22
6. TECHNICAL SECURITY CONTROLS 22
6.1 Key pair Generation and Installation 22
6.1.1 Key pair generation 22
6.1.2 Private Key delivery to Subscriber 22
6.1.3 Public key delivery to certificate issuer 22
6.1.4 CA public key delivery to Relying Parties 22
6.1.5 Key sizes 22
6.1.6 Public key parameters generation and quality checking 23
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 23
6.2 Private key protection and cryptographic module engineering controls 23
6.2.1 Cryptographic module standards and controls 23
6.2.2 Private Key (n out of m) multi-person control 23
6.2.3 Private Key escrow 23
6.2.4 Private Key backup 23
6.2.5 Private Key archival 23
6.2.6 Private Key transfer into or from a cryptographic module 23
6.2.7 Private Key storage on cryptographic module 23
6.2.8 Method of activating private key 23
6.2.9 Method of deactivating private key 23
6.2.10 Method of destroying private key 24
6.2.11 Cryptographic Module Rating 24
6.3 Other aspects of key pair management 24
6.3.1 Public key archival 24
6.3.2 Certificate operational periods and key pair usage periods 24
6.4 Activation data 24
6.4.1 Activation data generation and installation 24
6.4.2 Activation data protection 24
6.4.3 Other aspects of activation data 24
6.5 Computer security controls 24
6.5.1 Specific computer security technical requirements 24
6.5.2 Computer security rating 24
6.6 Life cycle technical controls 24

6.6.1 System development controls 24
6.6.2 Security management controls 24
6.6.3 Life cycle security controls 25
6.7 Network security controls 25
6.8 Time-stamping 25
7. CERTIFICATE, CRL AND OCSP PROFILES 25
7.1 Certificate profile 25
7.1.1 Version Numbers 25
7.1.2 Certificate Extensions 25
7.1.3 Algorithm Object Identifiers 25
7.1.4 Name Forms 25
7.1.5 Name Constraints 26
7.1.6 Certificate Policy Object Identifier 26
7.1.7 Usage of Policy Constraints Extension 26
7.1.8 Policy Qualifiers Syntax and Semantics 26
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 26
7.2 CRL profile 26
7.2.1 Version Numbers 26
7.2.2 CRL and CRL Entry Extensions 26
7.3 OCSP Profile 26
7.3.1 Version Numbers 26
7.3.2 OCSP Extensions 26
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 27
8.1 Frequency or circumstances of assessment 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 27
9.1 Fees 27
9.1.1 Certificate issuance or renewal fees 27
9.1.2 Certificate access fees 27
9.1.3 Revocation or status information access fees 27
9.1.4 Fees for other services 27
9.1.5 Refund policy 27
9.2 Financial responsibility 27
9.2.1 Insurance coverage 28
9.2.2 Other assets 28
9.2.3 Insurance or warranty coverage for end-entities 28
9.3 Confidentiality of business information 28
9.4 Privacy of personal information 28
9.4.1 Privacy plan 28
9.4.2 Information treated as private 28
9.4.3 Information not deemed private 28
9.4.4 Responsibility to protect private information 28
9.4.5 Notice and consent to use private information 28
9.4.6 Disclosure pursuant to judicial or administrative process 28
9.4.7 Other information disclosure circumstances 29

9.5 Intellectual property rights 29
9.6 Representations and warranties 29
9.6.1 CA representations and warranties 29
9.6.2 RA representations and warranties 29
9.6.3 Subscriber representations and warranties 29
9.6.4 Relying Party representations and warranties 29
9.6.5 Representations and warranties of other participants 29
9.7 Disclaimers of warranties 29
9.8 Limitations of liability 29
9.9 Indemnities 29
9.10 Term and termination 30
9.10.1 Term 30
9.10.2 Termination 30
9.10.3 Effect of termination and survival 30
9.11 Individual notices and communications with participants 30
9.12 Amendments 30
9.13 Dispute resolution provisions 30
9.14 Governing law 30
9.15 Compliance with applicable law 30
9.16 Miscellaneous provisions 30
9.17 Other provisions 30
APPENDIX A. REFERENCES 31
APPENDIX B. CERTIFICATE PROFILES 32
B.1 Individual – Hardware (High Assurance) Signature/Authentication Certificate 32
B.2 Individual – Hardware (High Assurance) Encryption/Confidentiality Certificate 35
APPENDIX C. CRL FORMAT 37
APPENDIX D. LEVEL OF ASSURANCE MAPPING 38
D.1 Assurance Level 38
D.2 Risk Assessment 39

Table of Tables

Table 1 – Signature OIDs 25
Table 2 - Algorithm OIDs 25
Table 3 - References 31
Table 4 - Identity Signature/Authentication Certificate Profile 34
Table 5 – Identity Confidentiality Certificate Profile 36

1. INTRODUCTION

Certificate Policies (CPs) 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 and/or class of applications with common security requirements. A CP may be used by a Relying Party to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application.

This Certificate Policy (CP) identifies the rules to manage the New Zealand Government **Individual – Hardware (High Assurance) Identity** certificates. It includes 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 New Zealand Government PKI Certification Practice Statement (CPS), or documents referenced by the CPS. In general, the rules in this CP identify the minimum standards in terms of performance, security and/or quality.

The headings in this CP follow the framework set out in 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: the provisions of any applicable contract such as a Subscriber Agreement, Deed of Agreement or other relevant contract override the provisions of this CP. The provisions of this CP prevail over the provisions of CPS to the extent of any direct inconsistency. The provisions of CPS govern any matter on which this CP is silent. (Note: where sub titled sections of the framework provide no additional information to detail provided in the CPS they have not been further extrapolated in this document.)

This section identifies and introduces the set of provisions, and indicates the types of entities and applications applicable for this CP.

1.1 Overview

An ID-HAC is used to identify an individual who has an affiliation with the New Zealand Government (Staff member, 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
iii. Provide a digital signature, as an individual affiliated with the New Zealand Government.

There are only 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-HAC holder, other than confirming an affiliation with the New Zealand Government.

This CP only allows *Subscribers*' keys and certificates to reside on a hardware based *token* with an embedded cryptographic engine. Before being issued with a token, the applicant is required to undergo a face to face identity verification that complies with the *Evidence of Identity* (EOI) policy for an *Identity - Hardware* (*High Assurance) certificate*.

1.2 Document name and identification

The title for this CP is the "X.509 Certificate Policy for New Zealand Government Individual – Hardware (High Assurance) Certificates". The *Object Identifier* (OID) for this CP is **2.16.554.101.8.1.2.4.1**

{ joint-iso-itu-t (2) member-body (16) NZ (554) Govt (101) pki (8) certificate policy (1) individual (2) Hardware (4) Version (1)}

1.3 PKI Participants

1.3.1 Certification authorities

The *Certification Authority* (CA) that issues certificates under this CP is an accredited CA under the High Assurance category subordinate to the New Zealand Government *Root CA* (RCA).

1.3.2 Registration authorities

The Registration Authorities (RAs) that perform the registration function under this CP are accredited New Zealand Government RAs. For further information, see CPS.

1.3.3 Subscribers

A *Subscriber* is the individual whose name appears as the subject in a certificate having signed a *Subscriber Agreement*, asserting their use of the *private key*s and associated certificate will be in accordance with this CP. The RA must formally verify the identity of the Subscriber and their requirement for an ID-HAC. Subscribers include:

i. New Zealand Government personnel;
ii. Customer organisations and their employees;
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-HAC.

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-HAC 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.

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-HACs 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 the 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 authenticate to New Zealand Government assets and systems to which the Subscriber has the requisite privileges.
iii. To provide accountability and non-repudiation of ID-HAC Subscriber transactions or communications;
iv. To verify the integrity of a communication from a Subscriber to and a Relying Party; and
v. 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 for Identity – Hardware (High Assurance) 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 the organisations 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 Cogito Group 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 certification 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 both internal and external of the 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 Group email address, and the Microsoft User 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 Group name space.
iv. 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 organisations 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 organisations email address and:

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

3.1.3 Anonymity or pseudonymity of Subscribers

This CP prohibits using an anonymous or pseudonymous Subscriber name.

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 organisations 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 New Zealand Government or subscribing organisations.

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

Following authentication of the Subscriber by a *Registration Officer* (RO), a token is issued to the Subscriber. The token generating the private and *public keys* submits a digitally signed certificate request to the RA. The RA validates the certificate request prior to submitting it to the CA for issuance.

To activate key usage, the Subscriber must enter their token's passphrase, thereby proving the Subscriber has possession of the token with the generated private key.

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 organisations Directory.

3.2.3 Authentication of individual identity

The RO, on behalf of the RA, must verify a Subscriber's identity before issuing a certificate and token. This must:

i. Occur face to face;
ii. Involve the presentation of EOI documents as required by the EOI policy for High Assurance Identity certificates (see http://www.pki.govt.nz/policy); and
iii. Total evidence presented must meet the following requirements:

    a) the applicant's name is on every document. Where the EOI documents bear a different name, then the linkage between that EOI document, the name to be registered and the applicant must be clearly established;
    b) the applicant's current address is on at least one of the documents;
    c) the applicant's signature is on at least one of the documents;
    d) the applicant's date of birth is on at least one of the documents; and
    e) a recognisable photograph of the applicant is on at least one of the documents.

iv. Authentication requires a handwritten signature on a Subscriber Agreement, which includes an affirmation that their identity matches the documentation presented.

The authentication process provides an audit record containing at a minimum:

i. The identity of the applicant;
ii. Document types, name as on document, and document unique identifier which were presented as EOI;
iii. The identity of the RO;

iv. The CA name and serial numbers of certificates issued, or the reason for rejection of application; and
v. The Subscriber's executed Subscriber Agreement.

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

All Subscribers will have their affiliation to their organisation verified, prior to issue of a certificate by the subscriber's organisation.

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

The minimum requirements for identification and authentication for a *re-key* are as follows:

i. A face to face presentation of the Subscriber to the RO is required for all re-keys;
ii. A Subscriber's affiliation shall be verified prior to performing a re-key; and
iii. The RO verifies the Subscriber's identity.

Verification of the Subscriber's identity can occur as follows:

i. As per initial enrolment; or
ii. Use of a Lead Agency approved biometric. (Only if a biometric was recorded during initial enrolment); or
iii. Proof of possession, and ability to exercise, a current private key, in which the DN matches a Government issued photographic ID document. This method can only be used provided no more than 4 years has passed since the Subscriber has been identified using the High Assurance requirements for EOI, or uses an approved biometric.

The Lead Agency may approve alternative methods to verify a Subscriber's identity for special circumstances. These circumstances include:

i. If such individuals do not have sufficient EOI documentation due to loss, theft or destruction of EOI documentation; or
ii. Individuals who for, legitimate reasons, have not been issued sufficient EOI documentation.

Certificates issued under special circumstances will require authorisation by the Lead Agency based on the risks associated with the circumstances. This authorisation will impose a limit on the reuse of the method by the Subscriber before reverting to standard method of verification (listed above). In addition, such certificates will have a defined validity period that is less than the normal certificate life of two years.

3.3.2 Identification and authentication for re-key after revocation

Re-key after revocation shall occur in the same manner as for initial identity validation, or the use of a Lead Agency approved biometric (only if the biometric was recorded during the initial enrolment).

3.4 Identification and authentication for revocation request

Revocation of certificates is in accordance with this section and 4.9 (Certificate revocation and suspension) of this CP and the CPS.

An *Authentication Services (AS) operator* or RO must verify the identity and authority of a requestor before carrying out a revocation on behalf of someone else.

Revocation requests can be authenticated in the following ways:

i. By digitally signed email; or
ii. By hand signed fax or letter; or
iii. In person, as per 3.3.1 (Identification and authentication for routine re-key).

In exceptional or emergency circumstances, a verbal revocation request can be processed at the discretion of *Operations Manager* or the Lead Agency.

The relationship to the Subscriber for revocation requests by the Subscriber's chain of command are to be verified via the Directory.

Subscribers may request a certificate's revocation via email or a 'self-service' web page, using that certificate's private key, regardless of the compromise status of the private key. A Subscriber has the authority, and requires no reasons, to submit a request to revoke their certificate.

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

i. The identity of the requestor;
ii. The reason for requesting revocation;
iii. The identity of the RO; and
iv. The issuing CA name and serial numbers of the certificates authorised for revocation, or the reason for rejecting the revocation request.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Any individual who has an approved affiliation with the New Zealand Government, and has a valid requirement, can submit an application for a certificate. Such an application can only be submitted via the accredited RA.

An individual's affiliation is determined by the subscriber's organisation.

4.1.2 Enrolment process and responsibilities

Upon receiving a request to issue a certificate to a Subscriber, the RA must ensure that each certificate application undergoes:

i. Confirmation of approval for the individual to hold a certificate;
ii. Validation of all information to be included in certificate request; and
iii. Confirmation of the individual's identity before issuing a token.

The Subscriber is required to present their EOI to an RO for verification. The RO then confirms affiliation and upon verifying the EOI registers the Subscriber application with the RA.

The RA forwards valid certificate requests to the CA for actioning.

The CA actions requests after confirming that the certificate request originated from an accredited RA and the details in the certificate request conforms with the CP profile for the requested certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

A summary of the process is as follows:

i. The RO verifies the affiliation and identity of the Subscriber at a face to face interview, as per requirements outlined in section 3.2 (Initial identity validation).
ii. The Subscriber signs the Subscriber Agreement.
iii. The RO enters identifying information for the Subscriber into the applicable certificate application form in the PKI software.
iv. The Subscriber token, keys and certificates are issued either at the time of enrolment, or at a later stage – see section 4.3 (Certificate Issuance).

4.2.2 Approval or rejection of certificate applications

A RO may reject or approve a certification application. Reasons for rejection could include insufficient affiliation, or the provision of incorrect or insufficient identification details.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

Depending on the facilities available to the RO, a token can be issued to the Subscriber at the time of enrolment or at a later stage:

Option 1 – Issuance at the time of enrolment:

If the enrolment is done at a facility where the RO is able to personalise hard tokens, the keys and certificates are issued at the time of enrolment. The *PKI software* initiates the private and public authentication key generation on the Subscriber's hard token.

If confidentiality keys are required, the private and public confidentiality keypair are generated in an approved cryptographic module and then stored on the Subscriber's hard token. A copy of the confidentiality private key is also encrypted.

The Subscriber enters a passphrase to protect the private key(s) on the token.

Option 2 – Issuance at a later date:

If the enrolment is done at an RO facility without token personalisation capability, the hard token is personalised centrally and securely delivered to the Subscriber, who is then able to access the PKI software to exercise private and public authentication key usage on the token using their passphrase.

In either case, the public keys for the Subscriber are validated by an RA and sent to the CA to be digitally signed. The signed certificates are returned and stored on the Subscriber's hard token.

4.3.1 CA actions during certificate issuance

See CPS.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

Notification to the Subscriber occurs for a certificate request either when it succeeds or fails.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Subscriber is deemed to have accepted a certificate when they have signed the Subscriber Agreement and *exercised* the private key.

4.4.2 Publication of the certificate by the CA

The New Zealand Government 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 above in 1.3.3 (Subscribers) and in the Subscriber Agreement.

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) details the Relying Party public key and certificate usage and responsibilities.

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

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

This CP permits certificate *renewal*.

The criteria for certificate *renewal* is 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

Subscribers shall be notified when a "renewal" certificate has been issued, and of any requirements necessary to update the Subscribers token.

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. Loss or compromise of a current private key requires revocation.

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

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

The Lead Agency receives notification of progress, issues and completion of Lead Agency initiated certificate re-keying activities.

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

4.8.1 Circumstance for certificate modification

The circumstances permitted for certificate *modification* include (but may not be limited to):

i. Details in the certificate relevant to the Subscriber have changed or been found to be incorrect (however if changes need to be made to subject name or email, the certificate must be revoked and re-issued); and

ii. Interoperation with approved "Third Party" PKI, or New Zealand Government assets and systems, require certificate attributes or contents inserted, modified or deleted.

The Lead Agency will determine other circumstances as appropriate.

4.8.2 Who may request certificate modification

Certificate modification may be requested by the:

i. Lead Agency, or
ii. Subscriber.

4.8.3 Processing certificate modification requests

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

4.8.4 Notification of new certificate issuance to Subscriber

The Subscriber receives notification when issued a modified certificate, or if rejection of a modification request occurs.

The Lead Agency receives notification of progress, issues and completion of Lead Agency initiated certificate modifications.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.8.6 Publication of the modified certificate by the CA

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

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The CPS defines circumstances for revocation.

4.9.2 Who can request revocation

See CPS.

4.9.3 Procedure for revocation request

Subscribers can request revocation of their own certificates at any time using email or a self-service web page.

Revocation requests received by AS operators or ROs 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 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.

4.11 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

All Subscribers use hard token technology to generate and securely store private authentication keys, with passphrase access controls. The individual receiving the hard token is responsible for the security and usage of this hard token. Under no circumstances will copies of private authentication keys be kept, or be capable of recovery.

Private confidentiality keys, if issued, must be generated in an approved cryptographic module and inserted into the token. Private encryption keys are always encrypted in transit to a level commensurate with that of the key itself.

See CPS for more detail.

6.1.2 Private Key delivery to Subscriber

Private authentication keys are always generated within the hard token.

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

Where private keys are generated on the Subscriber's token at the time of enrolment, no additional delivery process is required.

Where the token is not personalised at the time of enrolment, it will be securely delivered to the Subscriber. Activation information will be delivered separately and securely, using a mechanism for both deliveries that ensures that the private key(s) can only be accessed by the correct Subscriber.

6.1.3 Public key delivery to certificate issuer

While outside of the Subscriber's token, public keys are protected using an algorithm and process approved by GCSB.

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)

Keys issued under this CP 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.

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

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.

6.2.7 Private Key storage on cryptographic module

See CPS.

6.2.8 Method of activating private key

Activating private keys occurs by the Subscriber authenticating to the cryptographic module. The session stays live until deactivated (see 6.2.9).

6.2.9 Method of deactivating private key

Deactivation can be achieved via:

i. Shut down or restart of the system;

ii. Removal of the token; or
iii. Shut down of the service that operates the token.

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.

6.4 Activation data

6.4.1 Activation data generation and installation

When the certificate and associated key pairs are installed on the hard token during the certificate issuance, the Subscriber is requested to insert a passphrase. This passphrase is used as the activation data and must be in accordance with New Zealand Government policy, which complies with the NZISM.

Lifecycle management of passphrases and other activation data is in accordance with the Key Management Plan (KMP) and New Zealand Government policy.

6.4.2 Activation data protection

All passphrases used to activate the private key shall be kept in accordance with New Zealand Government policy.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

See CPS.

6.5.2 Computer security rating

See CPS.

6.6 Life cycle technical controls

6.6.1 System development controls

See CPS.

6.6.2 Security management controls

See CPS.

6.6.3 Life cycle security 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 Numbers

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 Policy 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 Policy 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

ID-HA Certificates issued under this policy shall assert this CP's OID:

{2.16.554.101.8.1.2.4.1}

Certificates issued under this policy shall also assert the appropriate LoA OID and, to enable the use of the certificate at lower Levels of Assurance, this policy enables the additional assertion of the lower (or 'stacked') LoA OIDs. LoA OIDs able to be asserted under this policy include:

{2.16.554.101.8.2.1.3.1} Level of Assurance – High (Individual)

{2.16.554.101.8.2.1.2.1} Level of Assurance – Medium (Individual)

{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 policy 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 Numbers

CRLs shall be X.509 version 2.

7.2.2 CRL and CRL Entry Extensions

See Appendix C.

7.3 OCSP Profile

7.3.1 Version Numbers

OCSP is implemented using version 1 as specified under RFC 6960.

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 coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

See CPS.

9.4 Privacy of personal information

9.4.1 Privacy plan

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 will sign a Subscriber Agreement agreeing to the terms and conditions of certificate use and acknowledging 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 will only retain details of Evidence of Identity (EOI) documentation presented and the unique document identifiers. This information is recorded in the RA and is protected in accordance with the requirements of the PKI Privacy statement.

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 Subscriber Agreement.

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

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, as part of signing the Subscriber Agreement, 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 Disclaimers 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 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 Cogito Group, available at http://www.pki.govt.nz/policy/CPS.pdf
[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/rfc6818.txt
[KMP]	New Zealand Government Public Key Infrastructure Key Management Plan (classified)
[RCA CP]	X.509 Certificate Policy for New Zealand Government Root Certification Authority and Subordinate Certificate Authorities, available at http://www.pki.govt.nz/policy
[VA CP]	X.509 Certificate Policy for Cogito Group 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 – Hardware (High Assurance) Signature/Authentication Certificate

Field	Critical	Identity Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within NZGOVT namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	

Issuer Distinguished Name		CN= NZGovtCA<Serial>
		OU= CAs
		OU= PKI
		O= Govt
		C= NZ
			Encoded as printable string.
			<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>	Maximum 2 years from date of issue.

Subject Distinguished Name		CN= <LHS of NZGOVT 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, rsaEncryption	
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 the issuing 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	Yes	digitalSignature nonrepudiation	
Extended key usage	No	{1.3.6.1.5.5.7.3.2} Microsoft Client Authentication {1.3.6.1.4.1.311.20.2.2} Microsoft Smart Card Logon {1.3.6.1.5.5.7.3.4} Secure email protection	
Private key usage period		Not Present	

Field	Critical	Identity Certificate Value	Notes
Certificate policies	No	[1] **2.16.554.101.8.1.2.4.1** Policy Qualifier – User Notice: ”Other than confirming affiliation with New Zealand Government, the New Zealand Government 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 this CP. UserNotice shall use explicitText field.
		[2] Policy OID: **{**2.16.554.101.8.2.1.3.1**}**	The LoA of this certificate can be one of the following depending on its alignment with the LoA requirements (refer to Annex D). 2.16.554.101.8.2.1.3.1 - Level of Assurance – High (Individual) 2.16.554.101.8.2.1.2.1- Level of Assurance – Medium (Individual) 2.16.554.101.8.2.1.1.1- Level of Assurance – Low (Individual)
		[3] Policy OID: {2.16.554.101.8.2.1.2.1}	Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above
		[4] Policy OID: {2.16.554.101.8.2.1.1.1}	Included to allow the certificate to be used in lower assurance contexts. Applicable OID will be below the OID expressed above
Policy Mapping		Not Present	
subject Alternative Name (Email)	No	<Organisations RFC822 email address>	Contains the Subject’s organisations principal email address.
Subject Alternative Name (Microsoft UPN)	No	<Organisations User Principal Name>	Contains the Subject’s organisations User 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 Points	No	[1] Distribution Point Name (http): http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl	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

Field	Critical	Identity Certificate Value	Notes
		[2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList	point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table 4 - Identity Signature/Authentication Certificate Profile

B.2 Individual – Hardware (High Assurance) Encryption/Confidentiality Certificate

Field	Critical	Identity Certificate Value	Notes
Version		V3 (2)	Version 3 of X.509
Serial		<octet string>	Must be unique within NZGOVT namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	

Issuer Distinguished Name		CN= NZGovtCA<Serial>
		OU= CAs
		OU= PKI
		O= Govt
		C= NZ
			Encoded as printable string.
			<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>	Maximum 2 years from date of issue

Subject Distinguished Name		CN= <LHS of organisations 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, rsaEncryption	
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 the issuing 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	Yes	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] **2.16.554.101.8.1.2.4.1** Policy Qualifier – User Notice: ”Other than confirming affiliation with New Zealand Government, the New Zealand Government 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 this CP. UserNotice shall use explicitText field.
		[2] Policy OID: **{**2.16.554.101.8.2.1.3.1**}**	Level of Assurance – High (Individual) The LoA of this certificate.

Field	Critical	Identity Certificate Value	Notes
		[3] Policy OID: {2.16.554.101.8.2.1.2.1}	Level of Assurance – Medium (Individual) Included to allow the certificate to be used in lower assurance contexts.
		[4] Policy OID: {2.16.554.101.8.2.1.1.1}	Level of Assurance – Low (Individual) Included to allow the certificate to be used in lower assurance contexts.
Policy Mapping		Not Present	
subject Alternative Name (Email)	No	<Organisation RFC822 email address>	Contains the Subjects organisation principal email address.
Subject Alternative Name (Microsoft UPN)	No	<Organisation RFC822 email address>	Contains the Subjects organisation principal email address.
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://www.govt.nz/pki/Certificates/NZGovtCA<serial>.crt
		[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}
		Access location: http://www.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 Points	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).

Table 5 – Identity Confidentiality Certificate Profile

Notes:
- This certificate may be renewed.
- Private keys bound to this certificate should be archived.

APPENDIX C. CRL FORMAT

Please refer to the issuing CA’s Certificate Policy.

APPENDIX D. LEVEL OF ASSURANCE MAPPING

D.1 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 PKI Levels of Assurance Requirements paper [LOA]:

CP's Highest Level of Assurance:	HIGH Assurance {**2.16.554.101.8.2.1.3.1**}. **As documented in section 7.1.6 above.**

REQUIREMENT	**CP'S MAPPING TO REQUIREMENT**
IDENTITY PROOFING	
EOI	The EOI is in accordance with the processes required for certification of a High Assurance certificate, as covered in section 3.2 above.
Evidence of Relationship	Subscriber must be identified in the organisation's directory, as covered in section 3.2.2 above.
Location	As documented in section 3.2.3 the location of the identity proofing must be local, and face-to-face.

CREDENTIAL STRENGTH	
Token Protection	As documented in section 6.2, the HA-CP token will be a hard token, which has been evaluated under Common Criteria and/or FIPS 140-2 and PIV 201. The keys will not be allowed to be exported, and the token will include the capability to identity tamper evidence.
Token Activation	As documented in section 6.4, the Subscriber is requested to insert a passphrase during token issuance. This passphrase is used as the activation data and must be in accordance with New Zealand Government passphrase policy. Lifecycle management of passphrases and other activation data is in accordance with the KMP and New Zealand Government Policy.
Life (Time) of Key Strength	The key strength is determined based on NIST SP 800-57-1. Refer to Annex B to determine the applicable algorithms and size. Use of RSA 2048 bit key size aligns the life of the key strength to the requirements for greater than seven (7) years, as required for High Assurance.

Certificate Management	
CA Protection	As documented within section 5, the CA protection is aligned with the High Assurance requirements.
Binding	As documented in section 4, the issuance of the AD-ID-HA certificate is tightly bound to the presentation of the EOI paperwork, during the presentation of the token storing the AD-ID-HA key pair. The issuance process is contiguous, and requires the identity of the Subscriber to be bound to their organisation email address.
Revocation (Publication)	As covered in section 4.9.7, the CRL is published every Operational day, day or at intervals no greater than once a week if there are no updates.
Compliance	The Compliance requirements are covered in the CPS and section 8. 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.

D.2 Risk Assessment

The issuances of certificates using the ID-HA Certificate Policy has been aligned with the New Zealand Government High Assurance, which should provide a relying party some assurance in the asserted identity.

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