

X.509 Certificate Policy

for the NZ Government

RSA Root Certificate Authority and

Subordinate Certificate Authorities

Version 0.8

6 May 2016

Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy, identified by subarcs of the object identifier **2.16.554.101.8.1.1.2.0.1** *for* RCA CP *and* **2.16.554.101.8.1.1.2.1.1** *for any* Policy CA and **2.16.554.101.8.1.1.2.2.1** for any Issuing CA *that is signed by the* RCA, 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 owned, approved and controlled by:** | NZ Government PKI (TaaS) Lead Agency - DIA |
| **The document owner authorises changes to be made to this document by:** | Cogito Group |

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Issue Date** | **Change / Amendment Description** | **Editor** |
| 0.1 Draft | Feb 2016 | Initial draft | SJL |
| 0.2 | Mar 2016 | Updates as per requirements from DIA/GCIO | 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 | 4 Apr 2016 | Review and Typos fixed, Updating AIA/CDP URLs | RB |
| 0.7 | 21 Apr 2016 | Review and updates from DIA/GCIO, incorporating lessons and changes from Key generation and signing Ceremony. | PA Cutforth  SJ Lillywhite |
| 0.8 | 6 May 2016 | DIA/GCIO and AoG Service Providers review |  |
| *1.0* | *May 2016* | *First formal public release (Issue)* |  |
|  |  |  |  |

**Signatures**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Appointment** | **Organisation** | **Name** | **Signature** | **Date** |
| Lead Agency SRO | DIA (CSD) | Chris Webb |  |  |
| AoG Enterprise Architect | DIA (GEA-NZ) | Phil Cutforth |  |  |
| Root CA Operations Manager | Cogito Group | Sean Lillywhite |  |  |

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 10

1.3.5 Other participants 10

1.4 Certificate usage 10

1.4.1 Appropriate certificate uses 10

1.4.2 Prohibited certificate uses 10

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 11

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 12

3.1.5 Uniqueness of names 12

3.1.6 Recognition, authentication, and role of trademarks 12

3.2 Initial identity validation 12

3.2.1 Method to prove possession of private key 12

3.2.2 Authentication of Organization Identity 13

3.2.3 Authentication of individual identity 13

3.2.4 Non-verified Subscriber information 13

3.2.5 Validation of authority 13

3.2.6 Criteria for interoperation 13

3.3 Identification and authentication for re-key requests 13

3.3.1 Identification and authentication for routine re-key 13

3.3.2 Identification and authentication for re-key after revocation 14

3.4 Identification and authentication for revocation request 14

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 14

4.1 Certificate application 14

4.1.1 Who can submit a certificate application 14

4.1.2 Enrolment process and responsibilities 14

4.2 Certificate application processing 14

4.2.1 Performing identification and authentication functions 14

4.2.2 Approval or rejection of certificate applications 15

4.2.3 Time to process certificate applications 15

4.3 Certificate issuance 15

4.3.1 CA actions during certificate issuance 15

4.3.2 Notification to Subscriber by the CA of issuance of certificate 15

4.4 Certificate acceptance 15

4.4.1 Conduct constituting certificate acceptance 15

4.4.2 Publication of the certificate by the CA 15

4.4.3 Notification of certificate issuance by the CA to other entities 15

4.5 Key pair and certificate usage 15

4.5.1 Subscriber private key and certificate usage 15

4.5.2 Relying Party public key and certificate usage 15

4.6 Certificate renewal 16

4.6.1 Circumstance for certificate renewal 16

4.6.2 Who may request renewal 16

4.6.3 Processing certificate renewal requests 16

4.6.4 Notification of new certificate issuance to Subscriber 16

4.6.5 Conduct constituting acceptance of a renewal certificate 16

4.6.6 Publication of the renewal certificate by the CA 16

4.6.7 Notification of certificate issuance by the CA to other entities 16

4.7 Certificate re-key 16

4.7.1 Circumstance for certificate re-key 16

4.7.2 Who may request certification of a new public key 16

4.7.3 Processing certificate re-keying requests 16

4.7.4 Notification of new certificate issuance to Subscriber 16

4.7.5 Conduct constituting acceptance of a re-keyed certificate 17

4.7.6 Publication of the re-keyed certificate by the CA 17

4.7.7 Notification of certificate issuance by the CA to other entities 17

4.8 Certificate modification 17

4.8.1 Circumstance for certificate modification 17

4.8.2 Who may request certificate modification 17

4.8.3 Processing certificate modification requests 17

4.8.4 Notification of new certificate issuance to Subscriber 17

4.8.5 Conduct constituting acceptance of modified certificate 17

4.8.6 Publication of the modified certificate by the CA 17

4.8.7 Notification of certificate issuance by the CA to other entities 17

4.9 Certificate revocation and suspension 18

4.9.1 Circumstances for revocation 18

4.9.2 Who can request revocation 18

4.9.3 Procedure for revocation request 18

4.9.4 Revocation request grace period 18

4.9.5 Time within which CA must process the revocation request 18

4.9.6 Revocation checking requirement for Relying Parties 18

4.9.7 CRL issuance frequency (if applicable) 18

4.9.8 Maximum latency for CRLs (if applicable) 18

4.9.9 On-line revocation/status checking availability 18

4.9.10 On-line revocation checking requirements 19

4.9.11 Other forms of revocation advertisements available 19

4.9.12 Special requirements re key compromise 19

4.9.13 Circumstances for suspension 19

4.9.14 Who can request suspension 19

4.9.15 Procedure for suspension request 19

4.9.16 Limits on suspension period 19

4.10 Certificate status services 19

4.11 End of subscription 19

4.12 Key escrow and recovery 19

4.12.1 Key escrow and recovery policy and practices 19

4.12.2 Session key encapsulation and recovery policy and practices 19

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 19

5.1 Physical controls 19

5.2 Procedural controls 19

5.3 Personnel controls 20

5.4 Audit logging procedures 20

5.5 Records archival 20

5.6 Key changeover 20

5.7 Compromise and disaster recovery 20

5.8 CA or RA termination 20

6. TECHNICAL SECURITY CONTROLS 20

6.1 Key pair generation and installation 20

6.1.1 Key pair generation 20

6.1.2 Private Key delivery to Subscriber 20

6.1.3 Public key delivery to certificate issuer 20

6.1.4 CA public key delivery to Relying Parties 20

6.1.5 Key sizes 21

6.1.6 Public key parameters generation and quality checking 21

6.1.7 Key usage purposes (as per X.509 v3 key usage field) 21

6.2 Private key protection and cryptographic module engineering controls 21

6.2.1 Cryptographic module standards and controls 21

6.2.2 Private Key (n out of m) multi-person control 21

6.2.3 Private Key escrow 21

6.2.4 Private Key backup 21

6.2.5 Private Key archival 21

6.2.6 Private Key transfer into or from a cryptographic module 22

6.2.7 Private Key storage on cryptographic module 22

6.2.8 Method of activating private key 22

6.2.9 Method of deactivating private key 22

6.2.10 Method of destroying private key 22

6.2.11 Cryptographic Module Rating 22

6.3 Other aspects of key pair management 22

6.3.1 Public key archival 22

6.3.2 Certificate operational periods and key pair usage periods 22

6.4 Activation data 22

6.4.1 Activation data generation and installation 22

6.4.2 Activation data protection 22

6.4.3 Other aspects of activation data 23

6.5 Computer security controls 23

6.6 Life cycle technical controls 23

6.7 Network security controls 23

6.8 Time-stamping 23

7. CERTIFICATE, CRL AND OCSP PROFILES 23

7.1 Certificate profile 23

7.1.1 Version Numbers 23

7.1.2 Certificate Extensions 23

7.1.3 Algorithm Object Identifiers 23

7.1.4 Name Forms 24

7.1.5 Name Constraints 24

7.1.6 Certificate Policy Object Identifier 24

7.1.7 Usage of Policy Constraints Extension 24

7.1.8 Policy Qualifiers Syntax and Semantics 24

7.1.9 Processing Semantics for the Critical Certificate Policies Extension 24

7.2 CRL profile 24

7.2.1 Version Numbers 24

7.2.2 CRL and CRL Entry Extensions 25

7.3 OCSP profile 25

7.3.1 Version Numbers 25

7.3.2 OCSP Extensions 25

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 25

8.1 Frequency or circumstances of assessment 25

8.2 Identity/qualifications of assessor 25

8.3 Assessor’s relationship to assessed entity 25

8.4 Topics covered by assessment 25

8.5 Actions taken as a result of deficiency 25

8.6 Communication of results 25

9. OTHER BUSINESS AND LEGAL MATTERS 25

9.1 Fees 25

9.1.1 Certificate issuance or renewal fees 25

9.1.2 Certificate access fees 25

9.1.3 Revocation or status information access fees 25

9.1.4 Fees for other services 26

9.1.5 Refund policy 26

9.2 Financial responsibility 26

9.2.1 Insurance coverage 26

9.2.2 Other assets 26

9.2.3 Insurance or warranty coverage for end-entities 26

9.3 Confidentiality of business information 26

9.4 Privacy of personal information 26

9.4.1 Privacy plan 26

9.4.2 Information treated as private 26

9.4.3 Information not deemed private 26

9.4.4 Responsibility to protect private information 26

9.4.5 Notice and consent to use private information 27

9.4.6 Disclosure pursuant to judicial or administrative process 27

9.4.7 Other information disclosure circumstances 27

9.5 Intellectual property rights 27

9.6 Representations and warranties 27

9.7 Disclaimers of warranties 27

9.8 Limitations of liability 27

9.9 Indemnities 27

9.10 Term and termination 27

9.10.1 Term 27

9.10.2 Termination 27

9.10.3 Effect of termination and survival 27

9.11 Individual notices and communications with participants 28

9.12 Amendments 28

9.13 Dispute resolution provisions 28

9.14 Governing law 28

9.15 Compliance with applicable law 28

9.16 Miscellaneous provisions 28

9.17 Other provisions 28

Appendix A. References 29

Appendix B. CERTIFICATE and CRL Profiles and FORMATS 30

B.1 RSA RCA Signature/Authentication Certificate 30

B.2 RSA RCA CRL 32

B.3 RSA POLICY CA SIGNATURE/AUTHENTICATION CERTIFICATE 33

B.4 RSA ISSUING CA SIGNATURE/AUTHENTICATION CERTIFICATE 35

B.5 RSA SUB-CA CRL 36

Table of Tables

[Table 1 – Signature OIDs 23](#_Toc450489417)

[Table 2 – Algorithm OIDs 23](#_Toc450489418)

[Table 3 – Level of Assurance OIDs 24](#_Toc450489419)

[Table 4 - References 29](#_Toc450489420)

[Table 5 – NZ Govt RSA Root Certification Authority Signature/Authentication Certificate Profile 31](#_Toc450489421)

[Table 6 – NZ Govt RSA Root CA CRL Profile 32](#_Toc450489422)

[Table 7 – Policy CA Signature/Authentication Certificate Profile 34](#_Toc450489423)

[Table 8 – Issuing CA Signature/Authentication Certificate Profile 36](#_Toc450489424)

[Table 9 – Sub-CA CRL Profile 37](#_Toc450489425)

# 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 and/or class of applications with common security requirements. A *Certificate Policy* (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 CP identifies the rules to manage the New Zealand Government. *RSA* *Root Certificate Authority* (RCA-RSA) certificates, *Subordinate Certificate Authority* (Sub-CA (Policy and Issuing)) certificates and associated *core component* 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 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 (IETF) Request for Comment (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. The content of this CP is based on the rules, requirements and architecture described in the New Zealand Government PKI Core Obligations Policy and the PKI Framework guide.

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 ‘New Zealand Government RSA Root Certification Authority and Subordinate CA Certificate Policy’ (NZ Government RCA-RSA and Sub-CA CP).

## Overview

The RCA is used to self-sign the Root CA certificate, digitally sign Policy-CA certificates to validate their properties, and sign and issue the certificates used by operational servers and operation personnel. The RCA is the highest point of trust within the New Zealand Government PKI hierarchy and all other CA and RA entities in the hierarchy rely on this trust anchor.

A Policy CA certificate is signed by the RCA and signs the certificates used by operational servers and operations personnel as well as signing the certificates issued to end-entities.

An Issuing CA certificate is signed by the Policy CA and signs the certificates used by operational servers and operations personnel as well as signing the certificates issued to end-entities.

This CP only allows the RCA and any Sub-CA (Policy or Issuing) private keys to reside on an approved[[1]](#footnote-1) Hardware Security Module (HSM). Any operations certificates required for PKI core components are required to be stored in accordance with the *Key Management Plan* (KMP).

Except for *Registration Officers* (RO) this CP allows *Operators’* keys and certificates to only reside on a hardware based *token* with an embedded cryptographic engine. Before issuing Operators’ keys and certificates, the applicant is required to perform a face-to-face identity verification that complies with the New Zealand Government PKI *Evidence of Identity* (EOI) policy for a *High Assurance certificate* and be cleared to the required level in accordance with the Service Providers *ICT Security Plan* (ICTSP).

## Document name and identification

The title for this CP is the “X.509 Certificate Policy for the New Zealand Government – Root Certificate Authority and Subordinate Certificate Authorities”. The Object Identifier (OID) for the RCA CP is: 2.16.554.101.8.1.1.2.0.1

**{joint-iso-itu-t (2) country (16) nz (554) govt (101) pki (8) certificate policy (1) certificate authority (1) root (2) component (0) version (1)}**

In addition, this CP is issued for any Policy CA that is signed by the RCA. In these circumstances, the OID is: 2.16.554.101.8.1.1.2.1.1

**{ joint-iso-itu-t (2) country (16) nz (554) govt (101) pki (8) certificate policy (1) certificate authority (1) root (2) subordinate policy (1) version (1)}**

In addition, this CP is issued for any Issuing CA that is signed by a Policy CA. In these circumstances, the OID is: 2.16.554.101.8.1.1.2.2.1

**{ joint-iso-itu-t (2) country (16) nz (554) govt (101) pki (8) certificate policy (1) certificate authority (1) root (2) subordinate issuing (2) version (1)}**

## PKI participants

### Certification authorities

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

This CP relates to:

1. the self-signed RCA authentication certificates that the RCA issues to itself;
2. the authentication and confidentiality certificates signed by the RCA and issued to Sub-CAs;
3. the authentication and confidentiality certificates issued by the Sub-CAs for the core operational infrastructure, e.g. the Registration Authority (RA) server; and
4. all operator certificates used for the purpose of maintenance and issuance responsibilities, such as CA operators (CAO) and *Registration Officers* (ROs).

### 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.*

### Subscribers

No end-entity *Subscribers* are issued certificates under this CP.

Certificates issued by the RCA or Sub-CA to the operators of core components will not be used as a validation mechanism for that individual. All such certificates will only be valid for use within the PKI core components[[2]](#footnote-2).

An entity issued a certificate under this CP must have access, authority or privilege to New Zealand Government assets or systems. New Zealand Government assets and systems may act as a *Relying Party*, with respect to chain of trust aspects, having granted access, authority or privilege to an individual.

### Relying Parties

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

Relying Parties are bound by the relevant CP that an end-entity certificate is issued under.

### Other participants

Other participants include:

1. the Lead Agency – refer to the Certification Practice Statement (CPS) for their responsibilities which specifically include:
   1. review and approval of this CP;
   2. presiding over the PKI audit process;
   3. approving mechanisms and controls for the management of the accredited infrastructure (CA/RA);
   4. approval of operational standards and guidelines to followed.
2. *Accreditation agencies* – to provide independent assurance that the facilities, practices and procedures used to issue certificates comply with this CP, the CPS and other relevant documentation (policy and legal).
3. *Directory Service* providers – to provide a *repository* for certificates and certificate status information issued under this CP.

## Certificate usage

### Appropriate certificate uses

Certificates issued under this CP, in conjunction with their associated *private keys*, allow the RCA to:

1. self-sign the RCA certificate;
2. digitally sign a Sub-CA certificate;
3. sign the operational certificates required by the PKI, including OCSP responder;
4. Sign the CRL; and
5. sign its own internal log files.

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

1. digitally sign end-entity certificates;
2. digitally sign a certificate for any CA subservient to the Sub-CA;
3. sign the operational certificates required by the PKI; and
4. sign its own internal log files.

All other core component certificates will only be valid for use within the PKI and used for the authentication and confidentiality (as appropriate) of core component activities.[[3]](#footnote-3)

### Prohibited certificate uses

The prohibited uses for certificates issued under this CP are:

1. for the RCA, to sign certificates issued to end-entity Subscribers;
2. to sign the certificate of a non-Lead Agency approved CA;
3. to validate the identity of a *AS operator* (CMS ROs excepted); and
4. to establish a Sub-CA to conduct any transaction, or communication, which is any or all of the following:
   1. Unrelated to New Zealand Government business;
   2. Illegal or criminal[[4]](#footnote-4);
   3. Unauthorised;
   4. Unethical, or
   5. Contrary to New Zealand Government policy.

Engaging in a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the AS operators and the New Zealand Government disclaims any and all liability in such circumstances.

## Policy administration

### Organisation administering the document

See CPS.

### Contact person

See CPS.

### Authority determining CPS suitability for the policy

See CPS.

### CPS approval procedures

See CPS.

## 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 Appendix B.3 of the CPS also applies to this CP.

# PUBLICATION AND REPOSITORY RESPONSIBILITIES

## Repositories

See CPS.

## Publication of certification information

The New Zealand Government publishes the issuing CA certificate, and the issuing CA’s latest CRL in its repository. This information is available to Relying Parties both internal[[5]](#footnote-5) and external[[6]](#footnote-6) of the New Zealand Government subscribing agencies.

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

1. this CP;
2. the CP for any end entity certificates; and
3. the CPS.

## Time or frequency of publication

Published documentation is updated on approved changes.

New Zealand Government PKI CAs publish new certificates and CRLs as operationally required and authorised (see [4.9.7](#_CRL_issuance_frequency) and relevant CP).

## Access controls on repositories

See CPS.

# IDENTIFICATION AND AUTHENTICATION

## Naming

### Types of names

Every certificate issued under this CP:

1. must have a clear distinguishable and unique Distinguished Name (DN) in the certificate subjectName field;
2. the common name components of the name are unique to the PKI name space;
3. the DN will be approved by the Lead Agency;
4. the RCA DN must be composed of NZGovtCA<Serial>; and
5. the Sub-CAs DN must be composed of NZGovtCA<Serial>.

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

### Need for names to be meaningful

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

### Anonymity or pseudonymity of Subscribers

Not applicable.

### Rules for interpreting various name forms

No stipulation as there is only one form.

### Uniqueness of names

Names are unique within the New Zealand Government PKI name space.

### Recognition, authentication, and role of trademarks

See CPS.

## Initial identity validation

### Method to prove possession of private key

*Private Key* generation of critical PKI core components is performed using Evaluation Assurance Level **4 (**EAL4) and Federal Information Processing Standard Publication 140-3 (FIPS-140-3) approved Hardware Security Modules (HSMs). These private keys are generated internally which ensures that the private key is never exposed or accidentally released. To initiate the key generation process the CA operator must use the HSM in the presence of the required staff as dictated by the Key Management Plan (KMP).

All AS Operators (RCAOs, CAOs, ROs etc.) use hard token technology to generate and securely store private keys, with passphrase access controls. The key generation process requires the operator to enter their token’s passphrase thereby proving the operator has possession of the token with the generated private key. Where soft tokens are used, certificate requests are submitted to the CA via PKCS#10 requests where proof of possession of the private key is ensured as the *Key Pair* is generated at the time the certificate request is created.

### Authentication of Organization Identity

To establish the RCA or an accredited Sub-CA, the Lead Agency must grant approval prior to the key generation ceremony. The establishment of other New Zealand Government PKI Sub-CAs requires Lead Agency approval prior to key generation.

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

1. identification of the infrastructure element and applicable Key Custodian;
2. witnessed generation of public and private keys;
3. generation of certificates;
4. verification by the Key Custodian that the key generation process was successful; and
5. entry into the PKI Trusted Element Register of the applicable information concerning the newly generated key.

Before issuing certificates to AS Operators, the operator is required to perform a face-to-face identity verification that complies with the *Evidence of Identity* (EOI) policy for a High Assurance certificate and be cleared to a minimum level of Confidential.

### Authentication of individual identity

See CPS.

### Non-verified Subscriber information

Not applicable.

### Validation of authority

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

### Criteria for interoperation

See CPS.

## Identification and authentication for re-key requests

### Identification and authentication for routine re-key

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

Verification of the Operator’s identity will be in accordance with Level 3 of Identity Proof (LoIP3) and can occur as follows:

1. as per initial registration; or
2. use of a Lead Agency approved biometric. (Only if biometric was recorded during previous registration); or
3. proof of possession, and ability to exercise a current private key in which the DN matches a Federal or State Government issued photographic ID document. This method can only be used provided no more than 4 years has passed since the Operator has been identified using the EOI policy for a High Assurance certificates, or uses an approved biometric.

The Lead Agency may approve alternative methods to verify an operator’s identity for special circumstances. These circumstances include:

1. if such individuals do not have sufficient EOI documentation due to loss, theft or destruction of 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 operator 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.

### Identification and authentication for re-key after revocation

Re-key is not allowed after revocation for CAs.

For operators, Re-Key after revocation shall occur in the same manner as for initial identity validation.

## Identification and authentication for revocation request

Revocation of certificates is in accordance with this section and [4.9](#_Certificate_revocation_and) of this CP and the CPS.

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

The Lead Agency must approve all requests for revocation of New Zealand Government PKI CAs. Revocation of other PKI core components, including operator certificates, can be approved by the Operations Manager or the Security Officer (SO).

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

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

# CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## Certificate application

### Who can submit a certificate application

People affiliated with the New Zealand Government, either through direct employment or Subscriber organization, can submit a certificate application that is authorised by the agencies Subscriber Authority prior to RA Operatons[[7]](#footnote-7). Creation of CAs must be authorised by the Lead Agency. There is no subsequent submission of applications for the creation of PKI core components related to that CA.

### Enrolment process and responsibilities

The enrolment process and responsibilities are outlined in the Operations Manual and KMP.

## Certificate application processing

### Performing identification and authentication functions

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

1. confirmation of approval for RCA or Sub-CA creation; and
2. validation of all information to be included in the certificate.

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

### Approval or rejection of certificate applications

The Lead Agency approves or rejects CA certificate applications.

The agency Subscriber Authority may approve or reject for agency certificate applications.

### Time to process certificate applications

See Subscriber Agreement, but if not stipulated then processing of certificate applications will occur in a timely manner.

## Certificate issuance

### CA actions during certificate issuance

See CPS.

### Notification to Subscriber by the CA of issuance of certificate

Operators shall be notified when a certificate has been issued and of any requirements necessary to update the operator’s token.

## Certificate acceptance

### Conduct constituting certificate acceptance

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

### Publication of the certificate by the CA

The only certificates published will be the CA certificates. These will be published to the Certificate Publishing repository and external repositories as per the CPS.

### Notification of certificate issuance by the CA to other entities

No stipulation.

## Key pair and certificate usage

### Subscriber private key and certificate usage

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

Custodians shall protect private keys from access by other parties in accordance with the KMP and CPS.

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

### Relying Party public key and certificate usage

1.4 (Certificate Usage) and [1.3.4](#_Relying_Parties) (Relying Parties) detail the Relying Party public key and certificate usage and responsibilities.

The interpretation and compliance with extended key usage attributes, and any associated limitations on the use of the certificate and/or private key, is in accordance with RFC 6818.

## Certificate renewal

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

### Circumstance for certificate renewal

The CPS defines the criteria for certificate renewals.

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

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

### Who may request renewal

Same as per applications - see 4.1.1 (Who can submit a certificate application).

### Processing certificate renewal requests

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

### Notification of new certificate issuance to Subscriber

Operators shall be notified when a “renewal” certificate has been issued, and of any requirements necessary to update the operator’s token.

### Conduct constituting acceptance of a renewal certificate

See [4.4.1](#_Conduct_constituting_certificate) (Conduct constituting certificate acceptance).

### Publication of the renewal certificate by the CA

PKI core component renewed certificates will not be published.

### Notification of certificate issuance by the CA to other entities

Not applicable.

## Certificate re-key

### Circumstance for certificate re-key

See CPS for relevant circumstances. Loss or compromise of a current private key requires revocation.

### Who may request certification of a new public key

Certificate re-key requests are made by an operator or the Lead Agency.

### Processing certificate re-keying requests

The process for certificate re-keying is consistent with the enrolment process defined in 4.1 (Certificate Application), however identification and authentication complies with 3.3 (Identification and Authentication for Re-Key Requests).

### Notification of new certificate issuance to Subscriber

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

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

### Conduct constituting acceptance of a re-keyed certificate

See [4.4.1](#_Conduct_constituting_certificate) (Conduct constituting certificate acceptance).

### Publication of the re-keyed certificate by the CA

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

### Notification of certificate issuance by the CA to other entities

Not applicable.

## Certificate modification

### Circumstance for certificate modification

The circumstances permitted for certificate modification are:

1. details in the certificate relevant to the Operator have changed or been found to be incorrect;
2. interoperation with approved “Third Party” PKI, or New Zealand Government assets and systems, require certificate attributes or contents inserted, modified or deleted; or
3. the name or title of the Lead Agency changes.

The Lead Agency will determine other circumstances as appropriate.

### Who may request certificate modification

Certificate modification may be requested by:

1. the Lead Agency,
2. Operations Manager, or
3. Operator.

### Processing certificate modification requests

The process for certificate modification must comply with enrolment process defined in [4.1](#_Certificate_application) (Certificate Application). The identification and authentication procedures must comply with [3.3](#_Identification_and_authentication) (Identification and Authentication for Re-Key Requests).

If the modification request changes the certificate substantially, it must be approved by the Lead Agency.

### Notification of new certificate issuance to Subscriber

The AS operator or key custodian receives notification when issued a modified certificate, or if rejection of a modification request occurs.

The Lead Agency receives notification of requests, issues and completion of all certificate modifications[[8]](#footnote-8).

### Conduct constituting acceptance of modified certificate

See [4.4.1](#_Conduct_constituting_certificate) (Conduct constituting certificate acceptance)

### Publication of the modified certificate by the CA

See [4.4.2](#_Publication_of_the) (Publication of the certificate by the CA)

### Notification of certificate issuance by the CA to other entities

No stipulation.

## Certificate revocation and suspension

### Circumstances for revocation

See CPS.

The NZ Government PKI will not maintain a separate ARL; but will include all such details in the CRL.

### Who can request revocation

See CPS.

### Procedure for revocation request

Revocation requests for PKI core components are performed by an authorised Certificate Authority Operator (CAO) but must be validated by the Operations Manager prior to initiation. The Disaster Recovery and Business Continuity Plan (DRBCP) details the revocation process for the RCA and Sub-CA in the event of an emergency.

Revocation of New Zealand AoG RCA and Sub-CA certificates require Lead Agency approval.

Revocation of Agency Sub-CA certificates require approval of the Subscribing Party (through the Subscriber Authority).

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

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

### 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.

### Time within which CA must process the revocation request

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

### 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.

### CRL issuance frequency (if applicable)

CRLs for the RCA are published when a Sub-CA is revoked, or a new Sub-CA is established, or every 180 days; whichever is the shorter period.

CRLs for Sub-CAs under this CP are published on each certificate revocation or at intervals no longer than 24 hours if there are no updates.

### Maximum latency for CRLs (if applicable)

The maximum latency between the generation and publication of CRLs is 3 days.

### 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) (Repositories) and the certificates CRL Distribution Point for further information.

### On-line revocation checking requirements

No stipulation.

### Other forms of revocation advertisements available

See CPS.

### Special requirements re key compromise

No stipulation.

### Circumstances for suspension

This CP does not support certificate suspension.

### Who can request suspension

This CP does not support certificate suspension.

### Procedure for suspension request

This CP does not support certificate suspension.

### Limits on suspension period

This CP does not support certificate suspension.

## Certificate status services

See CPS.

## End of subscription

See CPS.

## Key escrow and recovery

### Key escrow and recovery policy and practices

Escrow, backup and archiving of private keys issued under this CP is permitted to enable the retrieval of keys in a disaster recovery situation. However, operator hard tokens shall not be backed up or cloned.

Escrow, backup and archiving is to be undertaken in accordance with the KMP.

Retrieval will be undertaken in accordance with the PKI DRBCP recovery policy and practices.

### Session key encapsulation and recovery policy and practices

Symmetric keys are not required to be escrowed.

# FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## Physical controls

See CPS.

## Procedural controls

See CPS.

## Personnel controls

See CPS.

## Audit logging procedures

See CPS.

## Records archival

See CPS.

## Key changeover

See CPS.

## Compromise and disaster recovery

See CPS.

## CA or RA termination

See CPS.

# TECHNICAL SECURITY CONTROLS

## Key pair generation and installation

### Key pair generation

Key pair generation is via a combination of product and processes approved by the Lead Agency. Key pair generation is in accordance with the KMP and as such:

1. critical core components (e.g. CA and RA) generate keys within a HSM;
2. operators generate keys within a hard token or using EAL4 accredited software; and
3. non-critical core components generate keys using EAL4 accredited software (and protect them within PKCS#12 files).

### Private Key delivery to Subscriber

Private key delivery is in accordance with the KMP.

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

RC keys are delivered on a PKCS#12 file, passphrase protected by the RO at the time of key generation.

### Public key delivery to certificate issuer

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

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

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

### CA public key delivery to Relying Parties

See CPS.

### Key sizes

Keys used for this CP are in accordance with the KMP and will use SHA2 for signing and RSA public key algorithm. The key sizes for:

1. RCA is a minimum of 4096 bits;
2. Sub-CAs and components, other than operators, are a minimum 4096 bits; and
3. Operators are a minimum 4096 bits.

### Public key parameters generation and quality checking

See CPS.

### Key usage purposes (as per X.509 v3 key usage field)

In addition to the key usage defined in [1.4](#_Toc161801076), certificates include key usage extension fields to specify the purposes for which the Certificate may be used and also to technically limit the functionality of the certificate when used with the PKI software.

Note that the CAs have key usages “Digital Signature” and “Non-Repudiation” for the purpose of signing their own log entries.

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

## Private key protection and cryptographic module engineering controls

### Cryptographic module standards and controls

All cryptographic modules used with PKI core components comply with the Common Criteria scheme Evaluation Assurance Level **4 (**EAL4) and US Federal Information Processing Standard Publication 140-3 (FIPS-140-3) requirements. Cryptographic modules should be listed on the New Zealand Government *Evaluated Products List* or approved for the uses intended in this CP by the Lead Agency and GCSB. The RCA Hardware Security Modules (HSMs) are assessed (tested) by GCSB prior to use. See CPS for handling and management controls for cryptographic modules.

### Private Key (n out of m) multi-person control

See CPS.

### Private Key escrow

Escrow of private keys is permitted for Sub-CAs and occurs in accordance with the KMP and the PKI DRBCP. Refer to CPS for escrow controls.

### Private Key backup

See CPS.

### Private Key archival

Private Key archival occurs in accordance with the KMP and the PKI DRBCP as follows:

* RCAOs when RCA database is archived;
* Sub-CAOs when Sub-CA database is archived;
* Registration Authority Operatrors (RAOs) when the RA database is archived;
* ;
* Audit logs when the CMS databse is archived.

Archival of end entity private authentication keys does not occur.

### Private Key transfer into or from a cryptographic module

See CPS.

### Private Key storage on cryptographic module

See CPS.

### Method of activating private key

Activating private keys occurs by the CAO or RAO authenticating to the cryptographic module. For HSMs it is activated with the applicable physical key in the remote *PIN Entry Device* (PED) or directly into the HSM. The session stays live until deactivated (see [6.2.9](#_Method_of_deactivating) - Method of deactivating private key).

### Method of deactivating private key

Deactivation can be achieved via:

1. shut down or restart of the system;
2. removal of the token; or
3. shut down of the service that operates the token.

### Method of destroying private key

See CPS.

### Cryptographic Module Rating

See [6.2.1](#_Cryptographic_module_standards) (Cryptographic module standards and controls).

## Other aspects of key pair management

### Public key archival

See CPS.

### Certificate operational periods and key pair usage periods

The RSA RCA certificate validity has a maximum period of 10 years at generation, as agreed between the Lead Agency and GCSB in order to limit the key lifetime of this legacy algorithm.

A Sub-CA certificate may have a validity period of up to 5 years.

Certificate lives and key pair usage for all other core components, other than Operators, complements the relevant CA they are associated with.

Operator certificates have a maximum validity period of two years.

## Activation data

### Activation data generation and installation

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

Other passphrases and PINs used within the PKI system are created by operators at the time of installation.

Lifecycle management of passphrases, passwords and PINs used in the system is in accordance with the KMP and NZISM.

### Activation data protection

All passphrases used to activate core components are kept in accordance with New Zealand Government policy and KMP.

### Other aspects of activation data

No stipulation.

## Computer security controls

See CPS.

## Life cycle technical controls

See CPS.

## Network security controls

See CPS.

## Time-stamping

See CPS.

# CERTIFICATE, CRL AND OCSP PROFILES

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

1. the New Zealand Government RSA Root Certificate Authority;
2. sub-CA certificates signed by the New Zealand Government RSA Root Certificate Authority;
3. certificates issued to the PKI core components supporting a CA, such as the Registration Authority; and
4. certificates issued to the operators of the above components to ensure their abilities to undertake administration activities.

## Certificate profile

### Version Numbers

All certificates are X.509 Version 3 certificates.

### Certificate Extensions

See Appendix B.

### 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.

|  |  |
| --- | --- |
| rsaEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1} |
| Id-ecPublicKey | {iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 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, CRLs and any other PKI product, including other forms of revocation such as OCSP responses.

### Name Forms

The Common Name (CN) component is based on the name assigned by the Lead Agency to the CA being created presented as a printable string.

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

### Name Constraints

Name constraints are not present.

### Certificate Policy Object Identifier

CA Certificates issued under this policy shall assert the OID **{2.16.554.101.8.1.1.2.0.1}** for RCA certificates or **{2.16.554.101.8.1.1.2.1.1}** for Policy certificates or **{2.16.554.101.8.1.1.2.2.1}** for Issuing certificates.

The RCA and Sub-CA certificates shall also assert the any Policy OID of {**2.5.29.32.0**}.

The Sub-CA certificate shall also assert the following OIDs representing *Levels of Assurance* (LoA)of certificates issued:

|  |  |  |  |
| --- | --- | --- | --- |
| Individual: | Low |  | 2.16.554.101.8.2.1.1.0.1 |
|  | Medium |  | 2.16.554.101.8.2.1.2.0.1 |
|  | High |  | 2.16.554.101.8.2.1.3.0.1 |
|  |  |  |  |
| Resources: | Low |  | 2.16.554.101.8.2.2.1.0.1 |
|  | Medium |  | 2.16.554.101.8.2.2.2.0.1 |
|  | High |  | 2.16.554.101.8.2.2.3.0.1 |

Table 3 – Level of Assurance OIDs

### Usage of Policy Constraints Extension

Policy constraints are not present.

### 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.

### 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.

## CRL profile

### Version Numbers

CRLs issued under this CP shall assert a version number as described in the X.509 standard (ISO/IEC-9594-8). CRLs shall assert Version 2.

### CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available in Appendix B.

## OCSP profile

### Version Numbers

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

### OCSP Extensions

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

# COMPLIANCE AUDIT AND OTHER ASSESSMENTS

## Frequency or circumstances of assessment

See CPS.

## Identity/qualifications of assessor

See CPS.

## Assessor’s relationship to assessed entity

See CPS.

## Topics covered by assessment

See CPS.

## Actions taken as a result of deficiency

See CPS.

## Communication of results

See CPS.

# OTHER BUSINESS AND LEGAL MATTERS

## Fees

### Certificate issuance or renewal fees

As per the TaaS catalogues.

### Certificate access fees

There is no fee for accessing Certificates from approved repositories.

### Revocation or status information access fees

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

### Fees for other services

See CPS regarding fees for access to this CP. No fee has been stipulated for other services that are not already included in the TaaS catalogues.

### Refund policy

See CPS.

## Financial responsibility

See CPS.

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

### Insurance coverage

No insurance is provided or implied by New Zealand Government for use of services under this CP.

### Other assets

No stipulation.

### Insurance or warranty coverage for end-entities

No stipulation.

## Confidentiality of business information

See CPS.

## Privacy of personal information

### Privacy plan

No Personal Information (as defined in the *Privacy Act 1993*) will be collected during the creation of the RCA or a Sub-CA but it will be collected for the issuance of Operator certificates. If personal information is gathered, the collection, use and disclosure of such information is governed in accordance with the CPS.

### Information treated as private

Not applicable for core components other than Operators. The PKI will only retain details of EOI documentation presented and the unique document identifiers. This information will be stored by the Security Officer in accordance with New Zealand Government requirements and protected in accordance with the requirements of the Privacy Act Principles. Personal Information of Operators will not be published outside of the PKI.

### Information not deemed private

Not applicable for core components other than Operators. By accepting their role as an Operator, an Operator acknowledges that their email address and name may be contained in their Operator certificate and may be disclosed.

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

### Responsibility to protect private information

See CPS.

### Notice and consent to use private information

Not applicable for core components other than Operators. Acknowledgement by the Operator to the use of Personal Information is provided during induction into the PKI.

### Disclosure pursuant to judicial or administrative process

See CPS.

### Other information disclosure circumstances

No stipulation

## Intellectual property rights

See CPS.

## Representations and warranties

See CPS.

Subscriber representations and warranties are not applicable.

## Disclaimers of warranties

See CPS.

## Limitations of liability

See CPS.

In addition, the Lead Agency is responsible for performing the security accreditation process of the PKI core components (RCA and GNet Policy CA) with due care, in adherence to published New Zealand Government Criteria and Policies[[9]](#footnote-9).

The Lead Agency is responsible for the approval and governance of the PKI Framework Approved Documents, though the New Zealand Government accepts no liability for any errors and/or omissions in the final Approved Documents.

## Indemnities

See CPS.

## Term and termination

### 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.

### Termination

See CPS.

### Effect of termination and survival

See CPS.

## Individual notices and communications with participants

See CPS.

## Amendments

See CPS.

## Dispute resolution provisions

See CPS.

## Governing law

See CPS.

## Compliance with applicable law

See CPS.

## Miscellaneous provisions

See CPS.

## Other provisions

No Stipulation.

1. References

The following documents are referenced in this CP:

|  |  |
| --- | --- |
| **Ref ID / Short Code** | **Description** |
| ITU X.509 (2012)  ISO/IEC-9594-8:2005 | IT-OSI: The Directory: Public-key and attribute certificate frameworks, available at <http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509> |
| RFC 6960 | RFC 6960 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> |
| RFC 3647 | RFC 3647 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> |
| RFC 6818 | RFC 6818 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> |
| CC EAL4  (ISO/IEC-15408:2009) | Common Criteria scheme Evaluation Assurance Level 4, available at <https://www.commoncriteriaportal.org/products/>,  ISO/IEC-15408-x:2009 Computer Security Certification |
| FIPS-140-3  (ISO/IEC 19790:2012) | Federal Information Processing Standard Publication 140-3, available at <http://csrc.nist.gov/groups/ST/FIPS140_3/> |
| CPS | X.509 Certification Practice Statement for the New Zealand Government PKI, available at <http://www.pki.govt.nz/policy/CPS.pdf> |
| EoI  LoA  LoIP | Levels of Assurance (LoA), and Evidence of Identity (EoI) Levels of Identity Proof (LoIP), contained in The New Zealand Government Public Key Infrastructure Core Obligations Policy document, available at <http://www.pki.govt.nz/policy/> |
| VA CP | X.509 Certificate Policy for the New Zealand Government Validation Authority Certificates, available at <http://www.pki.govt.nz/policy/CPs> |
| KMP | The New Zealand Government Authentication Services Key Management Plan |
| ICTSP | The New Zealand Government ICT Security Plan for the New Zealand Government Authentication Services |
| NZISM | The New Zealand Government Information Security Manual, available at <http://www.gcsb.govt.nz/publications/the-nz-information-security-manual/> |
| PSR | The New Zealand Government Protective Security Requirements, available at <https://www.protectivesecurity.govt.nz/> |
| [Privacy Act] | New Zealand Privacy Act 1993, available at <http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html> |

Table 4 - References

1. CERTIFICATE and CRL Profiles and FORMATS
   1. RSA RCA Signature/Authentication Certificate

| **Field** | **Critical** | **NZ Govt RSA Root Certificate Value** | **Notes** |
| --- | --- | --- | --- |
| Version |  | V3 (2) | Version 3 of X.509 |
| Serial |  | <octet string> | Must be unique within the NZ Govt PKI 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 “001”. |
| Validity Period |  | Not before <UTCtime>  Not after <UTCtime> | Maximum 10 years from date of issue |
| Subject Distinguished Name |  | CN= NZGovtCA<Serial>  OU= CAs  OU= PKI  O= Govt  C= NZ | Encoded as printable string. |
| Subject Public Key Information |  | Minimum 4096 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, Certificate signing, CRLsigning, Off-line CRL signing | Digital signature and non-repudiation key usages are only used for the signing of the CA’s own log entries. |
| Extended key usage |  | Not Present |  |
| Private key usage period |  | Not Present |  |
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.0.1}  Policy Qualifier - CPS pointer: <https://www.pki.govt.nz/policy/> | The OID of this CP (RCA) |
|  |  | [2] Policy OID: {2.5.29.32.0} | anyPolicy OID |
| Policy Mapping |  | Not Present |  |
| Subject Alternative Name |  | Not Present |  |
| Issuer Alternative Name |  | Not Present |  |
| Subject Directory Attributes |  | Not Present |  |
| Basic Constraints | Yes | CA=True, path length constraint=none |  |
| Name Constraints |  | Not Present |  |
| Policy Constraints |  | Not Present |  |
| Authority Information Access |  | Not Present |  |
| CRL Distribution Points |  | Not Present |  |

Table 5 – NZ Govt RSA Root Certification Authority Signature/Authentication Certificate Profile

* 1. RSA RCA CRL

See RFC 6818 for detailed syntax. The following table lists which fields are expected.

|  |  |  |  |
| --- | --- | --- | --- |
| **Field** | **Critical** | **NZ Govt RSA Root CA CRL Value** | **Notes** |
| Version |  | V2 (1) | X.509 Version 2 CRL profile |
| Issuer Signature Algorithm |  | SHA256WithRSAEncryption |  |
| Issuer Distinguished Name |  | CN= NZGovtCA<Serial>  OU= CAs  OU= PKI  O= Govt  C= NZ |  |
| thisUpdate |  | <UTCTime> |  |
| nextUpdate |  | <UTCTime> | Date by which the next CRL will be issued (at the latest. If a CA certificate is revoked, or a new CA generated, a CRL will be issued at that time) thisUpdate + 31 days |
| Revoked certificates list |  | 0 or more 2-tuple of certificate serial number and revocation date (in UTCTime) |  |
| CRL extensions |  |  |  |
| CRL Number | No | <Integer> |  |
| Authority Key Identifier | No | <Octet String> | The value of this field is the 256 bit SHA256 hash of the binary DER encoding of the CA public key information |
| CRL entry extensions |  |  |  |
| Invalidity Date | No | Optional | Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. |
| Reason Code | No | Optional |  |

Table 6 – NZ Govt RSA Root CA CRL Profile

* 1. RSA POLICY CA SIGNATURE/AUTHENTICATION CERTIFICATE

| **Field** | **Critical** | **NZ Govt RSA Policy Certification Authority Certificate Value** | **Notes** | |
| --- | --- | --- | --- | --- |
| Version |  | V3 (2) | Version 3 of X.509 | |
| Serial |  | <octet string> | Must be unique within the NZ Govt 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 “101”. | |
| Validity Period |  | Not before <UTCtime>  Not after <UTCtime> | Maximum 5 years from date of issue | |
| Subject Distinguished Name |  | CN= NZGovtCA<Serial>  OU= CAs  OU= PKI  O= Govt  C= NZ | Encoded as printable string. | |
| Subject Public Key Information |  | Minimum 4096 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, Certificate Signing, Off-line CRL Signing, CRL Signing | Digital signature and Non repudiation key usages only used for signing the CA’s own log entries. | |
| Extended key usage |  | Not Present |  | |
| Private key usage period |  | Not Present |  | |
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.1.1} (this CP/Sub-CAs)  Policy Qualifier - CPS pointer: <https://www.pki.govt.nz/policy/> | The OID of this CP (Policy CA) | |
|  |  | [2] Policy OID: {2.5.29.32.0} | OID for “anyPolicy” | |
|  |  | [3] Policy OID: {2.16.554.101.8.2.1.1.0.1} (Individual – Low Assurance) |  | |
|  |  | [4] Policy OID: {2.16.554.101.8.2.1.2.0.1} (Individual – Medium Assurance) |  | |
|  |  | [5] Policy OID: {2.16.554.101.8.2.1.3.0.1} (Individual - High Assurance) |  | |
|  |  | [7] Policy OID: {2.16.554.101.8.2.2.1.0.1} (Resource – Low Assurance) |  | |
|  |  | [8] Policy OID: {2.16.554.101.8.2.2.2.0.1} (Resource – Medium Assurance) |  | |
|  |  | [9] Policy OID: {2.16.554.101.8.2.2.3.0.1} (Resource – High Assurance) |  | |
| Policy Mapping |  | Not Present |  | |
| Subject Alternative Name |  | Not Present |  | |
| Issuer Alternative Name |  | Not Present |  | |
| Subject Directory Attributes |  | Not Present |  | |
| Basic Constraints | Yes | CA=True, Path length constraint=1 |  | |
| 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](http://cert.pki.govt.nz/Certificates/NZGovtCA%3cserial%3e.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](http://cert.pki.govt.nz/pki/Certificates/NZGovtCA%3cserial%3e.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 | Distribution Point:  [1] URL=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 reason field may 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 7 – Policy CA Signature/Authentication Certificate Profile

* 1. RSA ISSUING CA SIGNATURE/AUTHENTICATION CERTIFICATE

| **Field** | **Critical** | **NZ Govt RSA Issuing Certificate Authority Certificate Value** | **Notes** | |
| --- | --- | --- | --- | --- |
| Version |  | V3 (2) | Version 3 of X.509 | |
| Serial |  | <octet string> | Must be unique within the NZ Govt 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 5 years from date of issue | |
| Subject Distinguished Name |  | CN= NZGovtCA<Serial>  OU= CAs  OU= PKI  O= GOVT  C= NZ | Encoded as printable string. | |
| Subject Public Key Information |  | Minimum 4096 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, Certificate Signing, Off-line CRL Signing, CRL Signing | Digital signature and Non repudiation key usages only used for signing the CA’s own log entries. | |
| Extended key usage |  | Not Present |  | |
| Private key usage period |  | Not Present |  | |
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.2.1} (this CP/Sub-CAs)  Policy Qualifier - CPS pointer: <https://www.pki.govt.nz/policy/> | The OID of this CP (Sub-CA) | |
|  |  | [2] Policy OID: {2.5.29.32.0} | OID for “anyPolicy” | |
|  |  | [3] Policy OID: {2.16.554.101.8.2.1.1.0.1} (Individual – Low Assurance) |  | |
|  |  | [4] Policy OID: {2.16.554.101.8.2.1.2.0.1} (Individual – Medium Assurance) |  | |
|  |  | [5] Policy OID: {2.16.554.101.8.2.1.3.0.1} (Individual - High Assurance) |  | |
|  |  | [7] Policy OID: {2.16.554.101.8.2.2.1.0.1} (Resource – Low Assurance) |  | |
|  |  | [8] Policy OID: {2.16.554.101.8.2.2.2.0.1} (Resource – Medium Assurance) |  | |
|  |  | [9] Policy OID: {2.16.554.101.8.2.2.3.0.1} (Resource – High Assurance) |  | |
| Policy Mapping |  | Not Present |  | |
| Subject Alternative Name |  | Not Present |  | |
| Issuer Alternative Name |  | Not Present |  | |
| Subject Directory Attributes |  | Not Present |  | |
| Basic Constraints | Yes | CA=True, Path length constraint=0 |  | |
| 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](http://cert.pki.govt.nz/Certificates/NZGovtCA%3cserial%3e.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](http://cert.pki.govt.nz/pki/Certificates/NZGovtCA%3cserial%3e.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 | Distribution Point:  [1] URL=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 reason field may 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 8 – Issuing CA Signature/Authentication Certificate Profile

* 1. RSA SUB-CA CRL

See RFC 6818 for detailed syntax. The following table lists which fields are expected. This profile can be used for both Policy and Issuing CAs under this CP.

|  |  |  |  |
| --- | --- | --- | --- |
| **Field** | **Critical** | **NZ Govt RSA Sub-CA CA CRL Value** | **Notes** |
| Version |  | V2 (1) | X.509 Version 2 CRL profile |
| Issuer Signature Algorithm |  | SHA256WithRSAEncryption |  |
| Issuer Distinguished Name |  | CN= NZGovtCA<Serial>  OU= CAs  OU= PKI  O= Govt  C= NZ |  |
| thisUpdate |  | <UTCTime> |  |
| nextUpdate |  | <UTCTime> | Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time)  Policy CA: thisUpdate + 30 days  Issuing CA: thisUpdate + 10 days |
| Revoked certificates list |  | 0 or more 2-tuple of certificate serial number and revocation date (in UTCTime) |  |
| CRL extensions |  |  |  |
| CRL Number | No | <Integer> |  |
| Authority Key Identifier | No | <Octet String> | The value of this field is the 256 bit SHA256 hash of the binary DER encoding of the CA public key information |
| CRL entry extensions |  |  |  |
| Invalidity Date | No | Optional | Date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. |
| Reason Code | No | Optional |  |

Table 9 – Sub-CA CRL Profile

1. EAL-4+ and FIPS-140-3 compliant. [↑](#footnote-ref-1)
2. The exception to this rule is ROs using the *Card Management System* (CMS), who use their Individual - High Assurance certificate to log in to the CMS in conjunction with “Issuer” rights in the system. [↑](#footnote-ref-2)
3. NB. ROs operating the CMS use their Individual - High Assurance certificate to log in to the system. [↑](#footnote-ref-3)
4. Although synonyms; the intent is to distinguish between legal/regulatory/Act misuse and criminal (cyber crime) misuse. [↑](#footnote-ref-4)
5. ‘Internal’ refers to agencies Intranet facilities; including AoG Common Web Platform (CWP), Shared Workspaces and Public Sector Intranet (PSI). [↑](#footnote-ref-5)
6. ‘External’ refers to publically accessible websites; such as ict.govt.nz and pki.govt.nz. [↑](#footnote-ref-6)
7. Subscriber Certificates not in scope for this requirement. [↑](#footnote-ref-7)
8. No longer than quarterly reporting to Lead Agency of new Certificate issuance. [↑](#footnote-ref-8)
9. Principally the PSR and NZISM, but including industry PKI specific requirements as applicable. [↑](#footnote-ref-9)