Cogito Group

DIGITAL IDENTITY AND SECURITY

X.509 Certificate Policy
for the
New Zealand Government PKI
RSA Secure Communications Certificates

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 **2.16.554.101.8.1.3.9.1**, 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	Updates OIDs to include version extension	SJL
0.6	Apr 2016	Review and update minor typo errors	RB
0.7	Apr 2016	Update AIA/CDP/CP publication points	BB
0.8	Apr 2016	Review and minor updates	BF
1.0	Aug 2020	Review and minor updates	BF

Signatures

Appointment	Organisation	Signature
Operations Manager	Cogito Group	
Lead Agency	DIA	

Contents

List of Tables

1. INTRODUCTION

Certificate Policies (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 CP identifies the rules to manage the New Zealand Government PKI *Resource Certificates* that are used to establish secure communication sessions using *Secure Sockets Layer* (SSL) and related protocols, such as *Transport Layer Security* (TLS). 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

This CP only applies to certificates issued to *New Zealand Government resources* for the establishment of secure communication sessions using SSL or a related protocol, and does not apply to other non-individuals (organisations, resources or devices) or any individuals.

No authority, or privilege, applies to a resource by becoming an approved Secure Communications Resource Certificate holder, other than confirming ownership by the New Zealand Government.

The principal documents referenced by this CP are shown in Appendix A. The contents of a referenced document may be classified.

1.2 Document name and identification

The title for this CP is "X.509 Certificate Policy for New Zealand Government PKI Secure Communications Resource Certificates". The *Object Identifier* (OID) for this CP is 2.16.554.101.8.1.3.9.1

{ joint-iso-itu-t (2) member-body (16)NZ(554) Govt (101) pki (8) certificate policy (1) resource (3) SC (9) version (1)}

Extensions of this OID represent the certificate variants governed by this CP. They are identified in Appendix B.

1.3 PKI participants

1.3.1 Certification authorities

The *Certification Authorities* (CAs) that issue certificates under this CP are New Zealand Government - accredited. For further information, see CPS.

1.3.2 Registration authorities

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

1.3.3 Subscribers

Secure Communications Resource Certificates are only issued to non-person entities (NPE), not individuals.

In this document - and as allowed by the definition of Subscriber in the CPS - the Subscriber of a New Zealand Government PKI Secure Communications Resource Certificate may, depending on the context, refer to the NPE whose name appears as the subject in the certificate, or to the person or legal entity that applied for that Certificate.

In some instances, certain responsibilities of the Subscriber (person or legal entity) may be delegated to a Key Custodian. The Subscriber person or legal entity is fully responsible and accountable for the acts or omissions of its delegate.

1.3.4 Relying parties

See CPS.

1.3.5 Other participants

See CPS.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The appropriate use for a certificate issued under this CP, in conjunction with its associated private key, is to:

- enable the New Zealand Government Resource to establish secure communications using SSL or a related protocol, such as TLS.

1.4.2 Prohibited certificate uses

The prohibited uses for certificates issued under this CP are:

- validating any Resource to conduct any transaction, or communication, which is illegal, unauthorised, unethical, and/or unrelated to New Zealand Government business.

Engaging in prohibited certificate use is a breach of the responsibilities and obligations agreed to by the *Registration Officer* (RO).

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 (B.3) of the CPS also applies to this CP.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See CPS.

2.2 Publication of certificate information

See CPS.

2.3 Time or frequency of publication

See 4.9.7 for CRL issuance frequency. For further information, see CPS.

2.4 Access controls on repositories

See CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

A clear distinguishable and unique Distinguished Name (DN) must be present in the certificate Subject field.

3.1.2 Need for names to be meaningful

The Lead Agency shall ensure that the DN in subjectName field used to identify the Subject of a certificate is:

i. Meaningful; and
ii. Relates directly to an attribute or identifier of the Resource.

3.1.3 Anonymity of pseudonymity of Subscribers

Not applicable.

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 PKI name space.

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

Certificate requests submitted to the CA must be PKCS#10 formatted requests where proof of possession of the Private Key is ensured and that the Key Pair is generated at the time the certificate request is created.

3.2.2 Authentication of organisation identity

The RO is responsible for the resource being deployed. Authentication of organisation identity is therefore implicit in an RO's authorisation for registration of the resource with the PKI.

3.2.3 Authentication of individual identity

This CP is for a non-human resource, and not an individual. The identifying characteristics of the resource will be resource specific. The RO authenticates the identity of the resource during the approval of the certification request after checking that the information in the request is correct.

3.2.4 Non-verified subscriber information

All Subscriber information included in the certificate request is verified by the RO.

3.2.5 Validation of authority

Prior to the issue of a certificate, *affiliation* with the New Zealand Government or subscriber organisation is validated by the RO.

3.2.6 Criteria for interoperation

See CPS.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and authentication for routine re-key

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

See 3.2.2 (Authentication of organisation identity) and 3.2.3 (Authentication of individual identity).

3.4 Identification and Authentication for Revocation Requests

Dual authentication is required for all requests to *revoke* (either two ROs or one RO and an AS Operator). Prior to revocation, the request is verified and the requestor and reasons documented.

Revocation requests, from sources other than a RO, should be digitally signed. If that is not possible, then a signed letter should be sent by post or fax.

Revocation requests, from sources other than a RO, are authenticated by verifying that the request is signed by the person making the request, validating that the sender is affiliated with the New Zealand Government, and checking that the request contains all the correct and required information.

Only in extraordinary (emergency) circumstances can a revocation request be submitted verbally.

See 4.9 (Certificate revocation and suspension) for more information on revocation.

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.

4.1.2 Enrolment process and responsibilities

Using the resource's security functionality, the resource's administrator generates a key pair and submits a certificate request. The RO verifies the information in the request and then approves it for registration. The RA validates and signs the request, and sends it to the CA.

The resource's administrator is responsible for providing accurate information in an application for the correct certificate type. The RO is responsible for checking the accuracy of that information and verifying that the application is for a New Zealand Government resource prior to approval for registration.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The RA signs and forwards the certificate request to the CA after receiving registration approval from an RO and validating the request. The CA only certifies certificate requests that are signed by an accredited New Zealand Government PKI RA.

4.2.2 Approval or rejection of certificate applications

A RO may reject or approve a certificate application. Reasons for rejection may include invalid application, insufficient affiliation with the New Zealand Government or subscriber organisation, or the provision of incorrect or insufficient identification details.

4.2.3 Time to process certificate applications

See CPS.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

See CPS.

4.3.2 Notification to subscriber by the CA of issuance of certificate

See CPS. In addition, the RO advises the resource's administrator when the certificate is available to be retrieved for installation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Use of the certificate constitutes acceptance.

4.4.2 Publication of the certificate by the CA

See CPS.

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

Certificates issued under this CP are only issued to non-person entities (NPE), not individuals.

The Key Custodian must ensure that:

i. the private key is protected from access by other parties in accordance with the KMP;
ii. the private key is only used in accordance with the key usage parameters set in the certificate; and
iii. the private key is no longer used following expiration or revocation of the certificate.

4.5.2 Relying party public key and certificate usage

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

The interpretation and compliance with extended KeyUsage attributes, and any associated limitations on the use of the certificate and/or private key, is in accordance with RFC6181.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

See CPS for certificate renewal criteria.

Certificate *renewal* is only permitted in exceptional circumstances and must not be used to avoid certificate re-key or the associated identification and authentication processes. For further information, see CPS.

4.6.2 Who may request renewal

See CPS.

4.6.3 Processing certificate renewal requests

The processing of certificate renewal requests is consistent with the processing of new certificate requests, as detailed in 4.2.1 (Certificate application processing).

4.6.4 Notification of new certificate issuance to subscriber

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

4.6.5 Conduct constituting acceptance of a renewal certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.6.6 Publication of the renewal certificate by the CA

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

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

See CPS.

4.7.2 Who may request certification of a new public key?

See 4.1.1 (Who can submit a certificate application).

4.7.3 Processing certificate re-keying requests

Processing of certificate *re-key* requests is consistent with the processing of new certificate requests, as detailed in 4.2.1 (Certificate application processing).

4.7.4 Notification of new certificate issuance to subscriber

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

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.7.6 Publication of the re-keyed certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

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 certificate subject have changed or been found to be incorrect.
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.

See CPS for further information.

4.8.2 Who may request certificate modification

See 4.1.1 (Who can submit a certificate application).

4.8.3 Processing certificate modification requests

The process for certificate modification is consistent with 4.2 (Certificate application processing). 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

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

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 CPS.

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

See CPS.

4.9.2 Who can request revocation

See CPS.

4.9.3 Procedure for revocation request

Revocation requests are verified on receipt in accordance with 3.4 (Identification and authentication for revocation requests) 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

See CPS.

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

Certificate suspension is not supported under this CP.

4.9.14 Who can request suspension

Certificate suspension is not supported under this CP.

4.9.15 Procedure for suspension request

Certificate suspension is not supported under this CP.

4.9.16 Limits on suspension period

Certificate suspension is not supported under this CP.

4.10 Certificate status services

4.10.1 Operational characteristics

See CPS.

4.10.2 Service availability

See CPS.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

See CPS.

4.12 Key escrow and recovery

Keys will not 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

5.5.1 Types of records archived

See CPS.

5.5.2 Retention period for archive

See CPS.

5.5.3 Protection of archive

See CPS.

5.5.4 Archive backup procedures

See CPS.

5.5.5 Requirements for time-stamping of records

See CPS.

5.5.6 Archive collection system (internal or external)

No Stipulation.

5.5.7 Procedures to obtain and verify archive information

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

Keys are primarily generated locally within the resource during the requesting process. Where a key pair is generated on behalf of the resource, the generation occurs centrally by a *trusted* role and following the placement of the keys in the custody of the resource the copy of the key pair is destroyed.

6.1.2 Private key delivery to subscriber

Generally the key generation is performed within the resource so no delivery is required. Where keys are generated externally the private key is delivered to the subscriber within a protected container known as a PKCS#12 file. The PKCS#12 format ensures the private key data is encrypted, and is only accessible with the provision of an unlocking password.

Where resources are working in a failover configuration, cloning of the key pair and certificate is permitted. It is the Resource administrator's responsibility to ensure that they are installed in the correct location(s).

6.1.3 Public key delivery to certificate issuer

Where keys are generated within the Resource, its public key is provided to the CA in a PKCS#10 certificate request file signed with the corresponding private key.

6.1.4 CA public key delivery to relying parties

See CPS.

6.1.5 Key sizes

Key sizes will be a minimum of 2048 bit RSA modulus.

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 establish secure communication sessions using SSL or a related protocol. See Appendix B and CPS for further information.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

See CPS.

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

See CPS.

6.2.3 Private key escrow

Escrow of keys does not occur.

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 Key Custodian 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; or
ii. shut down of the service that exercises the private key.

6.2.10 Method of destroying private key

See CPS.

6.2.11 Cryptographic Module Rating

See CPS.

6.3 Other aspects of key pair management

6.3.1 Public key archival

See CPS.

6.3.2 Certificate operational periods and key pair usage periods

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

6.4 Activation data

6.4.1 Activation data generation and installation

No Stipulation.

6.4.2 Activation data protection

See CPS.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

See CPS.

6.6 Life cycle technical controls

See CPS.

6.7 Network security controls

See CPS.

6.8 Time-stamping

See CPS.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

All certificates are X.509 Version 3 certificates.

7.1.2 Certificate extensions

See Appendix B.

7.1.3 Algorithm object identifiers

Certificates under this CP will use one of the following OIDs for signatures.

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Table 1 - Signature OIDs

Certificates under this CP will use one of the following OIDs for identifying the algorithm for which the subject key was generated.

id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Table 2 - Algorithm OIDs

7.1.4 Name forms

See CPS and Appendix B for further information.

7.1.5 Name constraints

Name constraints are not present.

7.1.6 Certificate policy object identifier

Certificates issued under this CP shall assert this CPs OID (or an extension of it – See Appendix B for variants):

(2.16.554.101.8.1.3.9.1)

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

{2.16.554.101.8.2.2.2.1} Level of Assurance – Medium (Resource)

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

{2.16.554.101.8.2.2.1.1} Level of Assurance – Low (Resource).

See also Appendix B.

7.1.7 Usage of policy constraints extension

See Appendix B.

7.1.8 Policy qualifiers syntax and semantics

See Appendix B.

7.1.9 Processing semantics for the critical certificate policies extension

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

7.2 CRL profile

7.2.1 Version number(s)

CRLs issued shall be X.509 version 2.

7.2.2 CRL and CRL entry extensions

See Appendix C.

7.3 OCSP profile

7.3.1 Version Numbers

OSCP is implemented using version 1 as specified under 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

9.2.1 Insurance

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

See CPS.

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

See CPS.

9.4 Privacy of personal information

Resource Certificates pertain to non-person entities, not individuals, and do not contain any personal information (as defined in the Privacy Act 1993).

9.5 Intellectual property rights

See CPS.

9.6 Representations and warranties

See CPS.

9.6.1 CA representations and warranties

See CPS.

9.6.2 RA representations and warranties

See CPS.

9.6.3 Subscriber representations and warranties

As the trusted role responsible for the private keys, the relevant Key custodian warrants to:

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

9.6.4 Relying party representations and warranties

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.

9.6.5 Representations and warranties of other participants

No Stipulation.

9.7 Disclaimer of warranties

See CPS.

9.8 Limitations of liability

See CPS.

9.9 Indemnities

See CPS.

9.10 Term and termination

9.10.1 Term

This CP and any amendments shall become effective upon publication in the Repository and shall remain in effect until the notice of its termination is communicated by the New Zealand Government PKI on its web site or Repository.

9.10.2 Termination

See CPS.

9.10.3 Effect of termination and survival

See CPS.

9.11 Individual notices and communications with participants

See CPS.

9.12 Amendments

See CPS.

9.13 Dispute resolution provisions

See CPS.

9.14 Governing Law

See CPS.

9.15 Compliance with Applicable Law

See CPS.

9.16 Miscellaneous provisions

See CPS.

9.17 Other provisions

See CPS.

APPENDIX A. REFERENCES

The following documents are referenced in this CP:

[CPS]	X.509 Certification Practice Statement for the New Zealand Government, available at http://www.pki.govt.nz/policy/
[6960]	RFC6960 Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol (OCSP), Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc6960.txt
[3647]	RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc3647.txt
[6818]	RFC6818 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc6818.txt
[KMP]	New Zealand Government Public Key Infrastructure Key Management Plan (classified)
[LOA]	New Zealand Government Public Key Infrastructure Assurance Level Requirements document, available at http://www.pki.govt.nz/policy/
[RCA CP]	X.509 Certificate Policy 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 New Zealand Government Validation Authority Certificates, available at http://www.pki.govt.nz/policy
[Privacy Act]	New Zealand Privacy Act 1993 http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

Table 3 - References

APPENDIX B. CERTIFICATE PROFILES

NB. Variations 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 Accreditation Authority.

B.1 Variation 1: SecureComms_Standard_V1.0

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		<*octet string*>	Must be unique within the New Zealand Government 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>	2 years from date of issue
Subject distinguished name		cn=<*unique identifier*> ou=SecureComms ou=Devices ou=NZGovtCA<serial> ou=PKI o=GOVT c=NZ	<unique identifier> as determined by device. Note: This is an example only, actual distinguished names will describe the subscriber organisation
Subject public key information		2048 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
X.509 v3 extensions			
Authority key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of signing CA's public key
Subject key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of subject's public key
Key usage	Yes	digitalSignature keyEncipherment	
Extended key usage	No	serverAuth clientAuth	
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy Id: {2.16.554.101.8.1.3.9.1} Policy qualifier – CPS pointer: https://www.pki.govt.nz/policy	The OID of this CP (variant 1)
		[2] Policy OID: **{2.16.554.101.8.2.2.2.1}**	Level of Assurance – Medium (Resource)

Field	Critical	Value	Notes
			The Level of Assurance of this certificate
		[3] Policy OID: **{2.16.554.101.8.2.2.1.1}**	Level of Assurance – Low (Resource) Included to allow the certificate to be used in lower assurance context.
Policy mapping		-	Not Present
Subject Alternative Name		-	Not Present
Issuer alternative name		-	Not Present
Subject directory attributes		-	Not Present
Basic constraints			Not Present
Name constraints		-	Not Present
Policy constraints		-	Not Present
Authority information access	No	[1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt [2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c [3] Access method=OCSP {1.3.6.1.5.5.7.48.1}: Access location: http://ocsp.pki.govt.nz/	
CRL Distribution Point	No	[1] Distribution Point Name (http): http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl [2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table 4 – Certificate Profile – Variation 1 - SecureComms_Standard

B.2 Variation 2: NZGOVT_Dir_SSL _V1.0

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		<*octet string*>	Must be unique within the 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>	2 years from date of issue
Subject distinguished name		cn=<*unique identifier*> ou=DSAs ou=Config o=GOVT c=NZ	<unique identifier> as determined by device.
Subject public key information		20 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
X.509 v3 extensions			
Authority key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of signing CA's public key
Subject key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of subject's public key
Key usage	No	digitalSignature nonRepudiation keyEncipherment	
Extended key usage	No	serverAuth clientAuth	
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy Id: {2.16.554.101.8.1.3.9.1} Policy qualifier – CPS pointer: https://www.pki.govt.nz/policy	The OID of this CP (variant 2)
		[2] Policy OID: {2.16.554.101.8.2.2.2.1}	Level of Assurance – Medium (Resource) The Level of Assurance of this certificate
		[3] Policy OID: {2.16.554.101.8.2.2.1.1}	Level of Assurance – Low (Resource) Included to allow the certificate to be used in lower assurance context.
Policy mapping		-	Not Present
Subject Alternative Name		-	Not Present
Issuer alternative name		-	Not Present
Subject directory attributes		-	Not Present

Field	Critical	Value	Notes
Basic constraints		-	Not Present
Name constraints		-	Not Present
Policy constraints		-	Not Present
Authority information access		[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/	Not Present
CRL Distribution Point	No	[1] Distribution Point Name (http): http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl [2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table 5 – Certificate Profile – Variation 2 - NZGOVT_Dir_SSL

B.3 Variation 3: SecureComms_WebServer_V1.0

Field	Critical	Value	Notes
Version		V3 (2)	
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>	2 years from date of issue
Subject distinguished name		cn=<*unique identifier*>, ou=SecureComms ou=Devices ou=NZGovtCA<serial> ou=PKI o=Govt c=NZ	<unique identifier> as determined by device. Note: This is an example only, actual distinguished names will describe the subscriber organisation
Subject public key information		2048 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
X.509 v3 extensions			
Authority key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of signing CA's public key
Subject key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of Subject's public key
Key usage	No	DigitalSignature keyEncipherment dataEncipherment NonRepudiation	
Extended key usage		ServerAuthentication ClientAuthentication	
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy Id: {2.16.554.101.8.3.9.1} Policy qualifier – CPS pointer: https://www.pki.govt.nz/policy	The OID of this CP (variant 2)
		[2] Policy OID: **{2.16.554.101.8.2.2.2.1}**	Level of Assurance – Medium (Resource) The Level of Assurance of this certificate
		[3] Policy OID: **{2.16.554.101.8.2.2.1.1}**	Level of Assurance – Low (Resource)

Field	Critical	Value	Notes
			Included to allow the certificate to be used in lower assurance context.
Policy mapping		-	Not Present
Subject Alternative Name	No	DNS Name: <*Fully Qualified Hostname*> DNS Name: <*Unqualified Hostname*> DNS Name: <*Fully Qualified Alias Hostname*> DNS Name: <*Fully Qualified Alias Hostname*> DNS Name: <*Fully Qualified Alias Hostname*> DNS Name: <*Fully Qualified Alias Hostname*> DNS Name: <*Fully Qualified Alias Hostname*> DNS Name: <*Fully Qualified Alias Hostname*> DNS Name: <*Fully Qualified Alias Hostname*> DNS Name: <*Fully Qualified Alias Hostname*>	
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		[1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt [2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c [3] Access method=OCSP {1.3.6.1.5.5.7.48.1}: Access location: http://ocsp.pki.govt.nz/	
CRL Distribution Point	No	[1] Distribution Point Name (http): http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl [2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table 6 – Certificate Profile – Variation 3 - SecureComms_WebServer

B.4 Variation 4: SecureComms_ClientAuth_V1.0

This variation allows central key generation due to application limitations.

Field	Critical	Value	Notes
Version		V3 (2)	
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>	2 years from date of issue
Subject distinguished name		cn=<*unique identifier*>, ou= SecureComms ou= Devices ou= NZGovtCA <serial> ou= PKI o= Govt c= NZ	<unique identifier> as determined by device. Note: This is an example only, actual distinguished names will describe the subscriber organisation
Subject public key information		2048 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
X.509 v3 extensions			
Authority key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of signing CA's public key
Subject key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of subject's public key
Key usage	No	digitalSignature nonRepudiation keyEncipherment dataEncipherment	
Extended key usage	No	clientAuth	
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy Id: {2.16.554.101.8.1.3.9.1} Policy qualifier – CPS pointer: https://www.pki.govt.nz/policy	The OID of this CP (variant 4)
		[2] Policy OID: {2.16.554.101.8.2.2.2.1}	Level of Assurance – Medium (Resource) The Level of Assurance of this certificate
		[3] Policy OID: {2.16.554.101.8.2.2.1.1}	Level of Assurance – Low (Resource)

Field	Critical	Value	Notes
			Included to allow the certificate to be used in lower assurance context.
Policy mapping		-	Not Present
Subject Alternative Name		-	Not Present
Issuer alternative name		-	Not Present
Subject directory attributes		-	Not Present
Basic constraints		-	Not Present
Name constraints		-	Not Present
Policy constraints		-	Not Present
Authority information access	No	[1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt [2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c [3] Access method=OCSP {1.3.6.1.5.5.7.48.1}: Access location: http://ocsp.pki.govt.nz/	
CRL Distribution Point		[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	Not Present

Table 7 – Certificate Profile – Variation 4 - SecureComms_ClientAuth

B.5 Variation 5: SecureComms_OfficeCommunicationsServer_V1.0

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		*<octet string>*	Must be unique within the 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>	2 years from date of issue

Field	Critical	Value	Notes
Subject distinguished name		cn=<*unique identifier*> ou=SecureComms ou=Devices ou= NZGovtCA <serial> ou=PKI o=Govt c=NZ	<unique identifier> as determined by device. Note: This is an example only, actual distinguished names will describe the subscriber organisation
Subject public key information		2048 bit RSA key modulus	
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
X.509 v3 extensions			
Authority key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of signing CA's public key
Subject key identifier	No	<*octet string*>	256 bit SHA256 hash of binary DER encoding of subject's public key
Key usage	No	digitalSignature nonRepudiation keyEncipherment dataEncipherment	
Extended key usage	No	serverAuth	
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy Id: {2.16.554.101.8.1.3.9.1} Policy qualifier – CPS pointer: https://www.pki.govt.nz/policy	The OID of this CP (variant 5)
		[2] Policy OID: {2.16.554.101.8.2.2.2.1}	Level of Assurance – Medium (Resource) The Level of Assurance of this certificate
		[3] Policy OID: {2.16.554.101.8.2.2.1.1}	Level of Assurance – Low (Resource) Included to allow the certificate to be used in lower assurance context.
Policy mapping		-	Not Present
Subject Alternative Name	No	DNS Name: <*Fully Qualified Hostname*> DNS Name: <*Unqualified Hostname*> DNS Name: <*Fully Qualified Alias Hostname*>	
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	

Field	Critical	Value	Notes
		[2] Access method=CAIssuer {1.3.6.1.5.5.7.48.2}: Access location: http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c [3] Access method=OCSP {1.3.6.1.5.5.7.48.1}: Access location: http://ocsp.pki.govt.nz/	
CRL Distribution Point	No	[1] Distribution Point Name (http): http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl [2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).
Microsoft Certificate Template		Office Communications Server	

Table 8 – Certificate Profile – Variation 5 - SecureComms_OfficeCommunicationsServer

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 Government PKI Assurance Level Requirements paper [LOA]:

CP's Level of Assurance:	Medium Assurance (Resource) **{2.16.554.101.8.2.2.2.1}**. As documented in section 7.1.6 above.

REQUIREMENT	CP'S MAPPING TO REQUIREMENT
IDENTITY PROOFING	
EOI	A Registration Officer is responsible for the identification of a resource and the verification of a certificate request during the enrolment of a resource, as described in 4.1.2 (Enrolment process and responsibilities). The RO is a trusted role, and the RO has proven their affiliation with the New Zealand Government or subscriber organisation and identity as part of their enrolment.
Evidence of Relationship	By being configured for use on the New Zealand Government or subscriber organisation IE by a trusted administrator with the required access permissions, the resource is authorised for registration to the New Zealand Government PKI.
Location	The identification of a resource maybe local or remote.
CREDENTIAL STRENGTH	
Token Protection	Private and public key pairs are generated on the resource using a cryptographic software module which also provides protection for the soft token during its lifecycle. See 6.2 (Private key protection and cryptographic module engineering controls).
Token Activation	Access to the private key is protected by passphrase in accordance with the New Zealand Government security requirements.
Life (Time) of Key Strength	As documented in Appendix B, the Key Strength will be RSA 2048 and SHA256 which in accordance with NIST SP800-57-1
CERTIFICATE MANAGEMENT	
CA Protection	The CA is both physically and logically secure from the unauthorised access. The CA protection requirements are documented in the CPS and sections 5 and 6 of this CP.

REQUIREMENT	CP'S MAPPING TO REQUIREMENT
Binding	As documented in section 4 (Certificate Lifecycle Operational Requirements), the key generation and issuance of a certificate to a resource is carried out by trusted roles, using the cryptographic capability on the resource itself. While the issuance process is not necessarily contiguous, the certificate signing request binds the certificate to the private key generated on the resource. The certificate also has a subject name which contains an identifier determined by the resource (see Appendix B. Certificate Profiles).
Revocation (Publication)	As covered in section 4.9.7, the CRL is published weekly, or on a certificate revocation, which exceeds the requirements. This is as a result of issuing from the High Assurance CA.
Compliance	The Compliance requirements are covered in the CPS and section 8 (Compliance audit and other assessments). The New Zealand Government PKI environment is certified under the New Zealand Government accreditation program, to support the issuance of up to a High Assurance level.

D.2 Risk Assessment

The issuances of certificates using this Certificate Policy has been aligned with a New Zealand Government Medium Assurance.

There were no risks identified in the alignment of this Certificate Policy with the requirements for Medium Assurance.