INTERNAL AFFAIRS
Te Tari Taiwhenua

New Zealand Government

Cogito Group
DIGITAL IDENTITY AND SECURITY

# Schedule A
# CERTIFICATE and CRL Profiles and FORMATS

Version 1.4
29th June 2018

# Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy, identified by subarcs of the object identifier **2.16.554.101.8.1.1.2.1** *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 |

# Revisions (Change History)

| Version | Revision Date | Change / Amendment Description | Editor |
|---|---|---|---|
| 0.1 Draft | Feb 2018 | Document Creation | B. Fardig |

# Approvals

| Appointment | Organisation | Name | Signature | Date |
|---|---|---|---|---|
| **Lead Agency SRO/CISO** | DIA (CSD) | Chris Webb | | |
| **GCIO Technical Design Authority** | DIA (ST) | James Collier | | |
| **CA Operations Manager** | Cogito Group | Brad Fardig | | |

# References

See Appendix A for References.

# Contents



# Table of Tables

# 1. INTRODUCTION

This document provides the Certificate and CRL profiles for the NZ All of Government (AoG) PKI.

This document is referenced by:

- NZ_Govt_PKI-RCA-CP

# 2. RSA CERTIFICATE AND CRL PROFILES AND FORMATS

## 2.1 RSA Root CA (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><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA. starting at "001". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 10 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA<Serial><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br>As this is a Root CA, the Issuer and Subject Distinguished Name should be the same. |
| 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 | |

| Field | Critical | NZ Govt RSA Root Certificate Value | Notes |
|---|---|---|---|
| Private key usage period | | Not Present | |
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.0.1}<br>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 1 – NZ Govt RSA Root Certification Authority (RCA) Signature/Authentication Certificate Profile**

## 2.2 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><br>OU= CAs<br>OU= PKI<br>O= Govt<br>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 +180 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 2 – NZ Govt RSA Root CA CRL Profile**

## 2.3 RSA Shared 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><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA. starting at "001". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA<Serial><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents this CA. starting at "101". |
| 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 | |

| Field | Critical | NZ Govt RSA Policy Certification Authority Certificate Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.1.1} (this CP/Sub-CAs)<br>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: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [6] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location:<br>http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer {1.3.6.1.5.5.7.48.2}<br>Access location:<br>http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz/ | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>[2] Distribution Point Name (ldap): | 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 |

| Field | Critical | NZ Govt RSA Policy Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList | complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). |

**Table 3 – RSA Shared Policy CA Signature/Authentication Certificate Profile**

## 2.4 Inland Revenue (IR) RSA Policy CA Signature/Authentication Certificate

| Field | Critical | IR 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><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA, starting at "001".<br><br>Initial CA issued by NZGovtCA001 |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA<Serial><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents this CA, starting from "101". |
| 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 | | Not Present | |

| Field | Critical | IR RSA Policy Certification Authority Certificate Value | Notes |
|---|---|---|---|
| period | | | |
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.3.1} (this CP/SubCAs)<br>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: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [6] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location:<br>http://PKI.nsp.ird.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http:// PKI.nsp.ird.govt.nz<br>/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://PKI.nsp.ird.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http:/PKI.nsp.ird.govt.nz/crl/NZGovtCA<Serial>.crl | The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. |

| Field | Critical | IR RSA Policy Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | 2] Distribution Point Name (ldap): ldap:// PKI.nsp.ird.govt.nz /cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList | 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 4– IR RSA Policy CA Signature/Authentication Certificate Profile**

## 2.5 RSA Shared Subordinate 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><br>OU= CAs<br>OU= PKI<br>O= GOVT<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA starting at "101". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA<Serial><br>OU= CAs<br>OU= PKI<br>O= GOVT<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents this CA. starting from "301". |
| 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 | |

| Field | Critical | NZ Govt RSA Issuing Certificate Authority Certificate Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.2.1} (this CP/Sub-CAs)<br>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: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [6] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location:<br>http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer {1.3.6.1.5.5.7.48.2}<br>Access location:<br>http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz/ | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>[2] Distribution Point Name (ldap): | 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 |

| Field | Critical | NZ Govt RSA Issuing Certificate Authority Certificate Value | Notes |
|---|---|---|---|
| | | ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList | complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). |

**Table 5 – RSA Shared Issuing CA Signature/Authentication Certificate Profile**

## 2.6 Inland Revenue (IR) RSA Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | IR RSA Issuing 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><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "101". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA<Serial><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "301". |
| 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 | |

| Field | Critical | IR RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.4.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [6] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location:<br>http://PKI.nsp.ird.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http:// PKI.nsp.ird.govt.nz<br>/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://PKI.nsp.ird.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http:/PKI.nsp.ird.govt.nz/crl/NZGovtCA<Serial>.crl<br>2] Distribution Point Name (ldap): ldap:// PKI.nsp.ird.govt.nz | 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 |

| Field | Critical | IR RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | /cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList | complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). |

**Table 6 – Inland Revenue (IR) RSA CA Signature/Authentication Certificate Profile**

## 2.7 Ministry of Justice (MoJ) RSA Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | MoJ RSA Issuing 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= NZGovtCA101<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "101". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA304<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "301". |
| 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 | |

| Field | Critical | MoJ RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.5.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [6] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location:<br>http://cert.pki.govt.nz/Certificates/NZGovtCA<Serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http:// cert.pki.govt.nz<br>/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>2] Distribution Point Name (ldap): ldap:// dir.pki.govt.nz | 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 |

| Field | Critical | MoJ RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | /cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList | complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). |

**Table 7 – Ministry of Justice (MoJ) RSA CA Signature/Authentication Certificate Profile**

## 2.8 Statistics NZ RSA Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | Statistics NZ RSA Issuing 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= NZGovtCA101<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "101". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA305<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "301". |
| 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 | |

| Field | Critical | Statistics NZ RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.6.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [6] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location:<br>http://cert.pki.govt.nz/Certificates/NZGovtCA<Serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location:<br>http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>2] Distribution Point Name (ldap): | 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 |

| Field | Critical | Statistics NZ RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList | complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension). |

**Table 8 – Statistics NZ RSA CA Signature/Authentication Certificate Profile**

## 2.9 Ministry of Business Innovation, and Employment (MBIE) RSA Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | MBIE RSA Issuing 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= NZGovtCA101<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "101". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA306<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "301". |
| 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 | |

| Field | Critical | MBIE RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.7.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [6] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location:<br>http://cert.pki.govt.nz/Certificates/NZGovtCA<Serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http:// cert.pki.govt.nz<br>/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl | The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. |

| Field | Critical | MBIE RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | 2] Distribution Point Name (ldap): ldap:// dir.pki.govt.nz /cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList | 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 9 – MBIE RSA CA Signature/Authentication Certificate Profile**

## 2.10 New Zealand Customs Service (NZCS) RSA Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | MBIE RSA Issuing 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= NZGovtCA101<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "101". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA307<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "301". |
| 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 | |

| Field | Critical | MBIE RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| Certificate policies | No | [1] Policy OID: {2.16.554.101.8.1.1.2.8.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [6] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location:<br>http://cert.pki.govt.nz/Certificates/NZGovtCA<Serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location: http:// cert.pki.govt.nz<br>/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl | The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. |

| Field | Critical | MBIE RSA Issuing Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | 2] Distribution Point Name (ldap): ldap:// dir.pki.govt.nz /cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList | 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 10 – New Zealand Customs Service (NZCS) RSA CA Signature/Authentication Certificate Profile**

## 2.11 RSA Subordinate CA (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><br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | <Serial> denotes the number after "NZGovtCA" that represents the associated CA |
| 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)<br>Policy CA: thisUpdate + 30 days<br>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 11 – RSA Subordinate CA CRL Profile**

# 3. ECC CERTIFICATE AND CRL PROFILES AND FORMATS

## 3.1 ECC RCA Signature/Authentication Certificate

| Field | Critical | NZ Govt ECC 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 | | sha384ECDSA | |
| Issuer Distinguished Name | | CN= NZGovtCA002<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "001". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 10 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA002<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string. |
| Subject Public Key Information | | sha384ECDSA | ECC secp384r1<br>FIPS186-3 p-384 |
| Issuer Unique Identifier | | Not Present | |
| Subject Unique Identifier | | Not Present | |
| X.509 V3 extensions: | | | |
| Authority Key Identifier | No | <octet string> | 384 bit SHA384 hash of binary DER encoding of signing CA's public key |
| Subject Key Identifier | No | <octet string> | 384 bit SHA384 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: {2.16.554.101.8.1.1.1.0.1}<br>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 | | Not Present | |

| Field | Critical | NZ Govt ECC Root Certificate Value | Notes |
|---|---|---|---|
| Attributes | | | |
| 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 12 – NZ Govt ECC Root Certification Authority Signature/Authentication Certificate Profile**

## 3.2 ECC RCA CRL

See RFC6818 for detailed syntax. The following table lists which fields are expected.

| Field | Critical | NZ Govt ECC Root CA CRL Value | Notes |
|---|---|---|---|
| Version | | V2 (1) | X.509 Version 2 CRL profile |
| Issuer Signature Algorithm | | sha384ECDSA | |
| Issuer Distinguished Name | | CN= NZGovtCA<Serial><br>OU= CAs<br>OU= PKI<br>O= Govt<br>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) 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 384 bit SHA384 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 13 – NZ Govt ECC Root CA CRL Profile**

## 3.3 ECC Shared Policy CA Signature/Authentication Certificate

| Field | Critical | NZ Govt ECC 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 | | sha384ECDSA | |
| Issuer Distinguished Name | | CN= NZGovtCA002<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "301". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA 102<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string. |
| Subject Public Key Information | | Minimum 384bit ECC secp384r1 | |
| Issuer Unique Identifier | | Not Present | |
| Subject Unique Identifier | | Not Present | |
| X.509 V3 extensions: | | | |
| Authority Key Identifier | No | <octet string> | 384 bit SHA384 hash of binary DER encoding of the issuing CA's public key |
| Subject Key Identifier | No | <octet string> | 384 bit SHA384 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: {2.16.554.101.8.1.1.1.1.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |

| Field | Critical | NZ Govt ECC Policy Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | [9] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location:<br>http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>[2] Distribution Point Name (ldap):<br>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 14 – ECC Shared Policy CA Signature/Authentication Certificate Profile**

## 3.4 ECC Shared Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | NZ Govt ECC Sub-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 | | sha384ECDSA | |
| Issuer Distinguished Name | | CN= NZGovtCA102<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "301". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA 302<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string. |
| Subject Public Key Information | | Minimum 384bit ECC secp384r1 | |
| Issuer Unique Identifier | | Not Present | |
| Subject Unique Identifier | | Not Present | |
| X.509 V3 extensions: | | | |
| Authority Key Identifier | No | <octet string> | 384 bit SHA384 hash of binary DER encoding of the issuing CA's public key |
| Subject Key Identifier | No | <octet string> | 384 bit SHA384 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: {2.16.554.101.8.1.1.1.2.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |

| Field | Critical | NZ Govt ECC Sub-Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | [9] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location:<br>http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>2] Distribution Point Name (ldap):<br>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 15 – ECC Shared Issuing CA Signature/Authentication Certificate Profile**

## 3.5 Inland Revenue (IR) ECC Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | NZ Govt ECC Sub-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 | | sha384ECDSA | |
| Issuer Distinguished Name | | CN= NZGovtCA102<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "301". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA308<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string. |
| Subject Public Key Information | | Minimum 384bit ECC secp384r1 | |
| Issuer Unique Identifier | | Not Present | |
| Subject Unique Identifier | | Not Present | |
| X.509 V3 extensions: | | | |
| Authority Key Identifier | No | <octet string> | 384 bit SHA384 hash of binary DER encoding of the issuing CA's public key |
| Subject Key Identifier | No | <octet string> | 384 bit SHA384 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: {2.16.554.101.8.1.1.1.3.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |

| Field | Critical | NZ Govt ECC Sub-Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | [9] Policy OID: {2.16.554.101.8.2.2.3.1} (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}<br>Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location:<br>http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>2] Distribution Point Name (ldap):<br>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 16 – Inland Revenue (IR) ECC CA Signature/Authentication Certificate Profile**

## 3.6 Ministry for Primary Industries (MPI) ECC Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | NZ Govt ECC Sub-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 | | sha384ECDSA | |
| Issuer Distinguished Name | | CN= NZGovtCA102<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "301". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA309<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string. |
| Subject Public Key Information | | Minimum 384bit ECC secp384r1 | |
| Issuer Unique Identifier | | Not Present | |
| Subject Unique Identifier | | Not Present | |
| X.509 V3 extensions: | | | |
| Authority Key Identifier | No | <octet string> | 384 bit SHA384 hash of binary DER encoding of the issuing CA's public key |
| Subject Key Identifier | No | <octet string> | 384 bit SHA384 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: {2.16.554.101.8.1.1.1.4.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |

| Field | Critical | NZ Govt ECC Sub-Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | [7] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |
| | | [9] Policy OID: {2.16.554.101.8.2.2.4.1} (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}<br>Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location:<br>http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>2] Distribution Point Name (ldap):<br>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 17 –Ministry for Primary Industries (MPI) ECC CA Signature/Authentication Certificate Profile**

## 3.7 Oranga Tamariki (OT) ECC Subordinate Issuing CA Signature/Authentication Certificate

| Field | Critical | NZ Govt ECC Sub-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 | | sha384ECDSA | |
| Issuer Distinguished Name | | CN= NZGovtCA102<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string.<br><Serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "301". |
| Validity Period | | Not before <UTCtime><br>Not after <UTCtime> | Maximum 5 years from date of issue |
| Subject Distinguished Name | | CN= NZGovtCA310<br>OU= CAs<br>OU= PKI<br>O= Govt<br>C= NZ | Encoded as printable string. |
| Subject Public Key Information | | Minimum 384bit ECC secp384r1 | |
| Issuer Unique Identifier | | Not Present | |
| Subject Unique Identifier | | Not Present | |
| X.509 V3 extensions: | | | |
| Authority Key Identifier | No | <octet string> | 384 bit SHA384 hash of binary DER encoding of the issuing CA's public key |
| Subject Key Identifier | No | <octet string> | 384 bit SHA384 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: {2.16.554.101.8.1.1.1.5.1} (this CP/SubCAs)<br>Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/ | The OID of this CP (SubCA) |
| | | [2] Policy OID: {2.5.29.32.0} | OID for "anyPolicy" |
| | | [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance) | |
| | | [4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance) | |
| | | [5] Policy OID: {2.16.554.101.8.2.1.3.1} (Individual - High Assurance) | |
| | | [7] Policy OID: {2.16.554.101.8.2.2.1.1} (Resource – Low Assurance) | |
| | | [8] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance) | |

| Field | Critical | NZ Govt ECC Sub-Certification Authority Certificate Value | Notes |
|---|---|---|---|
| | | [9] Policy OID: {2.16.554.101.8.2.2.4.1} (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}<br>Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt<br>[2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2}<br>Access location:<br>http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7c<br>[3] Access method: OCSP {1.3.6.1.5.5.7.48.1}<br>Access location: http://ocsp.pki.govt.nz | |
| CRL Distribution Points | No | Distribution Point:<br>[1] URL=http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl<br>2] Distribution Point Name (ldap):<br>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 18 – Oranga Tamariki (OT) ECC CA Signature/Authentication Certificate Profile**

## 3.8 SUB-CA CRL

See RFC6818 for detailed syntax. The following table lists which fields are expected. This profile can be used for both policy or issuing CAs

| Field | Critical | NZ Govt ECC Sub-CA CA CRL Value | Notes |
|---|---|---|---|
| Version | | V2 (1) | X.509 Version 2 CRL profile |
| Issuer Signature Algorithm | | sha384ECDSA | |
| Issuer Distinguished Name | | CN= NZGovtCA<Serial><br>OU= CAs<br>OU= PKI<br>O= Govt<br>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)<br>Policy CA: thisUpdate + 30 days<br>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 384 bit SHA384 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 19 – Sub-CA CRL Profile**