





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	NZ Government PKI (TaaS) Lead Agency - DIA
by:	
The document owner authorises changes to be	Cogito Group
made to this document by:	

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.

Date	Filename	Page
22 March 2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	2 of 47



Contents

1. INTRODUCTION	N	5
2. RSA CERTIFICA	TE AND CRL PROFILES AND FORMATS	6
	(RCA) Signature/Authentication Certificate	
	L	
2.3 RSA Shared	Policy CA Signature/Authentication Certificate	9
2.4 Inland Reve	nue (IR) RSA Policy CA Signature/Authentication Certificate	12
2.5 RSA Shared	Subordinate Issuing CA Signature/Authentication Certificate	15
2.6 Inland Rever 18	nue (IR) RSA Subordinate Issuing CA Signature/Authentication Cert	tificate
2.7 Ministry of J	ustice (MoJ) RSA Subordinate Issuing CA Signature/Authentication	
Certificate		21
2.8 Statistics NZ	RSA Subordinate Issuing CA Signature/Authentication Certificate	24
2.9 Ministry of E	Business Innovation, and Employment (MBIE) RSA Subordinate Issu	ing CA
	ication Certificate	27
	and Customs Service (NZCS) RSA Subordinate Issuing CA	
	ication Certificate	
2.11 RSA Subor	rdinate CA (Sub-CA) CRL	33
3. ECC CERTIFICA	TE AND CRL PROFILES AND FORMATS	34
3.1 ECC RCA Sign	nature/Authentication Certificate	34
3.2 ECC RCA CRI	, 	36
3.3 ECC Shared I	Policy CA Signature/Authentication Certificate	37
3.4 ECC Shared S	Subordinate Issuing CA Signature/Authentication Certificate	39
3.5 Inland Reve	nue (IR) ECC Subordinate Issuing CA Signature/Authentication Cert	ificate
41		
3.6 Ministry for	Primary Industries (MPI) ECC Subordinate Issuing CA	
Signature/Authent	cication Certificate	43
_	ariki (OT) ECC Subordinate Issuing CA Signature/Authentication	
3.8 SUB-CA CRL		47
Table of Tables		
Table of Tables		
Table 1 - N7 Cout PSA	Root Certification Authority (RCA) Signature/Authentication Certificate	Drofila
Table 1 - NZ dovi NSA		
Table 2 – N7 Govt RSA	Root CA CRL Profile	
	Policy CA Signature/Authentication Certificate Profile	
	CA Signature/Authentication Certificate Profile	
	ssuing CA Signature/Authentication Certificate Profile	
	nue (IR) RSA CA Signature/Authentication Certificate Profile	
	istice (MoJ) RSA CA Signature/Authentication Certificate Profile	
	RSA CA Signature/Authentication Certificate Profile	
	A Signature/Authentication Certificate Profile	
	d Customs Service (NZCS) RSA CA Signature/Authentication Certificate	
	linate CA CRL Profile	
	C Root Certification Authority Signature/Authentication Certificate Profi	
	C Root CA CRL Profile	
	Policy CA Signature/Authentication Certificate Profile	
	Issuing CA Signature/Authentication Certificate Profile	
Tubic 13 – LCC silai eu	13341116 or 1 Signature/ rudicinication oct unicate i 101116	40
Date	Filename	Page
22 March 2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	iii of 47

DMS Reference: 4631155DA

New Zealand Government



Table 16 - Inland Revenue (IR) ECC CA Signature/Authentication Certificate Profile	42
Table 17 - Ministry for Primary Industries (MPI) ECC CA Signature/Authentication Certificate Pr	
	44
Table 18 - Oranga Tamariki (OT) ECC CA Signature/Authentication Certificate Profile	46
Table 19 – Sub-CA CRL Profile	47

Date	Filename	Page
22 March 2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	iv of 47
	DMS Reference: 4631155DA	



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

Date	Filename	Page
22 March 2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	5 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt PKI namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= NZGovtCA <serial> OU= CAs</serial>	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the issuing</serial>
		OU= PKI O= Govt	CA. starting at "001".
		C= NZ	
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 10 years from date of issue
Subject Distinguished		CN= NZGovtCA <serial></serial>	Encoded as printable string.
Name		OU= CAs OU= PKI	As this is a Root CA, the Issuer and Subject Distinguished Name should be the same.
		O= Govt C= NZ	
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=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	6 of 47



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} Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/	The OID of this CP (RCA)
Policy Manning		[2] Policy OID: {2.5.29.32.0} Not Present	anyPolicy OID
Policy Mapping 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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	7 of 47
	DMS Reference: 4631155DA	



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> OU= CAs OU= PKI O= Govt C= NZ</serial>	
thisUpdate		<utctime></utctime>	
nextUpdate		<utctime></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></integer>	
Authority Key Identifier	No	<octet string=""></octet>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	8 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= NZGovtCA <serial> OU= CAs OU= PKI O= Govt C= NZ</serial>	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the issuing CA. starting at "001".</serial>
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA <serial> OU= CAs OU= PKI O= Govt C= NZ</serial>	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents this CA. starting at "101".</serial>
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=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	9 of 47



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) 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} 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/</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl [2] Distribution Point Name (ldap):</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	10 of 47
	DMS Reference: 4631155DA	



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</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	11 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= NZGovtCA <serial> OU= CAs OU= PKI O= Govt C= NZ</serial>	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the issuing CA, starting at "001". Initial CA issued by NZGovtCA001</serial>
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA <serial> OU= CAs OU= PKI O= Govt C= NZ</serial>	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents this CA, starting from "101".</serial>
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=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	12 of 47



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) 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} Access location: http://PKI.nsp.ird.govt.nz/Certificates/NZGovtCA <serial>.crt [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://PKI.nsp.ird.govt.nz /pki/Certificates/NZGovtCA<serial>.p7c [3] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://PKI.nsp.ird.govt.nz</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http:/PKI.nsp.ird.govt.nz/crl/NZGovtCA <serial>.crl</serial>	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form.

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	13 of 47
	DMS Reference: 4631155DA	



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?certificateRev ocationList</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	14 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished		CN= NZGovtCA <serial></serial>	Encoded as printable string.
Name		OU= CAs	<serial> denotes the number after "NZGovtCA" that represents the issuing</serial>
		OU= PKI	CA starting at "101".
		O= GOVT	
		C= NZ	
Validity Period		Not before <utctime></utctime>	Maximum 5 years from date of issue
		Not after <utctime></utctime>	
Subject Distinguished		CN= NZGovtCA <serial></serial>	Encoded as printable string.
Name		OU= CAs	<serial> denotes the number after "NZGovtCA" that represents this CA.</serial>
		OU= PKI	starting from "301".
		O= GOVT	
		C= NZ	
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	No	<octet string=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Identifier			
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	15 of 47



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) 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} 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/</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl [2] Distribution Point Name (ldap):</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	16 of 47
	DMS Reference: 4631155DA	



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</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	17 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished		CN= NZGovtCA <serial></serial>	Encoded as printable string.
Name		OU= CAs	<serial> denotes the number after "NZGovtCA" that represents the Issuing</serial>
		OU= PKI	CA starting at "101".
		0= Govt	
		C= NZ	
Validity Period		Not before <utctime></utctime>	Maximum 5 years from date of issue
		Not after <utctime></utctime>	
Subject Distinguished		CN= NZGovtCA <serial></serial>	Encoded as printable string.
Name		OU= CAs	<serial> denotes the number after "NZGovtCA" that represents the Issuing</serial>
		OU= PKI	CA starting at "301".
		0= Govt	
		C= NZ	
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	No	<octet string=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Identifier			
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	18 of 47



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) 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} Access location: http://PKI.nsp.ird.govt.nz/Certificates/NZGovtCA <serial>.crt [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http:// PKI.nsp.ird.govt.nz /pki/Certificates/NZGovtCA<serial>.p7c [3] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://PKI.nsp.ird.govt.nz</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http:/PKI.nsp.ird.govt.nz/crl/NZGovtCA <serial>.crl 2] Distribution Point Name (ldap): ldap:// PKI.nsp.ird.govt.nz</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	19 of 47
	DMS Reference: 4631155DA	



Field	Critical	IR RSA Issuing Certification Authority Certificate Value	Notes
		/cn=NZGovtCA <serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRev ocationList</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	20 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished		CN= NZGovtCA101	Encoded as printable string.
Name		OU= CAs	<serial> denotes the number after "NZGovtCA" that represents the Issuing</serial>
		OU= PKI	CA starting at "101".
		0= Govt	
		C= NZ	
Validity Period		Not before <utctime></utctime>	Maximum 5 years from date of issue
		Not after <utctime></utctime>	
Subject Distinguished		CN= NZGovtCA304	Encoded as printable string.
Name		OU= CAs	<serial> denotes the number after "NZGovtCA" that represents the Issuing</serial>
		OU= PKI	CA starting at "301".
		0= Govt	
		C= NZ	
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	No	<octet string=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Identifier			
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	21 of 47



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) 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} 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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl 2] Distribution Point Name (ldap): ldap:// dir.pki.govt.nz</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	22 of 47
	DMS Reference: 4631155DA	



Field	Critical	MoJ RSA Issuing Certification Authority Certificate Value	Notes
		/cn=NZGovtCA <serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRev ocationList</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	23 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= NZGovtCA101 OU= CAs OU= PKI O= Govt C= NZ	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "101".</serial>
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA305 OU= CAs OU= PKI O= Govt C= NZ	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "301".</serial>
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=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	24 of 47
	DMS Reference: 4631155DA	



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) 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} 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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl 2] Distribution Point Name (ldap):</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	25 of 47
	DMS Reference: 4631155DA	



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

Table 8 - Statistics NZ RSA CA Signature/Authentication Certificate Profile

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	26 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= NZGovtCA101 OU= CAs OU= PKI O= Govt C= NZ	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "101".</serial>
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA306 OU= CAs OU= PKI O= Govt C= NZ	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "301".</serial>
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=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	27 of 47
	DMS Reference: 4631155DA	



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) 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} 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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl</serial>	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form.

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	28 of 47
	DMS Reference: 4631155DA	



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?certificateRev ocationList</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	29 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		SHA256WithRSAEncryption	
Issuer Distinguished Name		CN= NZGovtCA101 OU= CAs OU= PKI O= Govt C= NZ	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "101".</serial>
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA307 OU= CAs OU= PKI O= Govt C= NZ	Encoded as printable string. <serial> denotes the number after "NZGovtCA" that represents the Issuing CA starting at "301".</serial>
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=""></octet>	256 bit SHA256 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	30 of 47
	DMS Reference: 4631155DA	



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) 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} 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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl</serial>	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form.

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	31 of 47
	DMS Reference: 4631155DA	



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?certificateRev ocationList</serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	32 of 47
	DMS Reference: 4631155DA	



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> OU= CAs OU= PKI O= Govt C= NZ</serial>	<serial> denotes the number after "NZGovtCA" that represents the associated CA</serial>
thisUpdate		<utctime></utctime>	
nextUpdate		<utctime></utctime>	Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time) Policy CA: thisUpdate + 30 days Issuing CA: thisUpdate + 10 days
Revoked certificates list		0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)	
CRL extensions			
CRL Number	No	<integer></integer>	
Authority Key Identifier	No	<octet string=""></octet>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	33 of 47



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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	34 of 47
	DMS Reference: 4631155DA	



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		Not Present	
Access			
CRL Distribution Points		Not Present	

Table 12 - NZ Govt ECC Root Certification Authority Signature/Authentication Certificate Profile

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	35 of 47
	DMS Reference: 4631155DA	



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> OU= CAs OU= PKI O= Govt C= NZ</serial>	
thisUpdate		<utctime></utctime>	
nextUpdate		<utctime></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></integer>	
Authority Key Identifier	No	<octet string=""></octet>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	36 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		sha384ECDSA	
Issuer Distinguished Name		CN= NZGovtCA002 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".</serial>
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA 102 OU= CAs OU= PKI O= Govt 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=""></octet>	384 bit SHA384 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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.} (this CP/SubCAs) 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)	
	1		
		[8] Policy OID: {2.16.554.101.8.2.2.2.1} (Resource – Medium Assurance)	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	37 of 47



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} 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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl [2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ? certificateRevocationList</serial></serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	38 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		sha384ECDSA	
Issuer Distinguished Name		CN= NZGovtCA102 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".</serial>
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA 302 OU= CAs OU= PKI O= Govt 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=""></octet>	384 bit SHA384 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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) Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/	The OID of this CP (SubCA)
		[2] Policy OID: {2.5.29.32.0} [3] Policy OID: {2.16.554.101.8.2.1.1.1} (Individual – Low Assurance)	OID for "anyPolicy"
		[4] Policy OID: {2.16.554.101.8.2.1.2.1} (Individual – Medium Assurance)	
	1	[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)	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx DMS Reference: 4631155DA	39 of 47



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} 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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl 2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ? certificateRevocationList</serial></serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	40 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		sha384ECDSA	
Issuer Distinguished		CN= NZGovtCA102	Encoded as printable string.
Name		OU= CAs OU= PKI	<serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "301".</serial>
		O= Govt C= NZ	
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA308 OU= CAs OU= PKI O= Govt	Encoded as printable string.
		C= NZ	
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=""></octet>	384 bit SHA384 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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) 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)	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	41 of 47
	DMS Reference: 4631155DA	



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} 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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl 2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ? certificateRevocationList</serial></serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	42 of 47
	DMS Reference: 4631155DA	



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

Field	Critical	NZ Govt ECC Sub-Certification Authority Certificate	Notes
		Value	
Version		V3 (2)	Version 3 of X.509
Serial		<octet string=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		sha384ECDSA	
Issuer Distinguished		CN= NZGovtCA102	Encoded as printable string.
Name		OU= CAs	<serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is</serial>
		OU= PKI	expected to start at "301".
		0= Govt	
		C= NZ	
Validity Period		Not before <utctime></utctime>	Maximum 5 years from date of issue
		Not after <utctime></utctime>	
Subject Distinguished		CN= NZGovtCA309	Encoded as printable string.
Name		OU= CAs	
		OU= PKI	
		O= Govt	
		C= NZ	
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=""></octet>	384 bit SHA384 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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)	The OID of this CP (SubCA)
		Policy Qualifier - CPS pointer: https://www.pki.govt.nz/policy/	
		[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)	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	43 of 47
	DMS Reference: 4631155DA	



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: CAlssuer{1.3.6.1.5.5.7.48.2} Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA <serial>.crt [2] Access method: CAlssuer{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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl 2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ? certificateRevocationList</serial></serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	44 of 47
	DMS Reference: 4631155DA	



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=""></octet>	Must be unique within the NZ Govt namespace
Issuer Signature Algorithm		sha384ECDSA	
Issuer Distinguished		CN= NZGovtCA102	Encoded as printable string.
Name		OU= CAs OU= PKI	<serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "301".</serial>
		O= Govt C= NZ	
Validity Period		Not before <utctime> Not after <utctime></utctime></utctime>	Maximum 5 years from date of issue
Subject Distinguished Name		CN= NZGovtCA310 OU= CAs OU= PKI O= Govt 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=""></octet>	384 bit SHA384 hash of binary DER encoding of the issuing CA's public key
Subject Key Identifier	No	<octet string=""></octet>	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) 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)	

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	45 of 47
	DMS Reference: 4631155DA	



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} 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</serial></serial>	
CRL Distribution Points	No	Distribution Point: [1] URL=http://crl.pki.govt.nz/crl/NZGovtCA <serial>.crl 2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ? certificateRevocationList</serial></serial>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	46 of 47
	DMS Reference: 4631155DA	



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> OU= CAs OU= PKI O= Govt C= NZ</serial>	
thisUpdate		<utctime></utctime>	
nextUpdate		<utctime></utctime>	Date by which the next CRL will be issued (at the latest – if a certificate is revoked, a CRL will be issued at that time) Policy CA: thisUpdate + 30 days Issuing CA: thisUpdate + 10 days
Revoked certificates list		0 or more 2-tuple of certificate serial number and revocation date (in UTCTime)	
CRL extensions			
CRL Number	No	<integer></integer>	
Authority Key Identifier	No	<octet string=""></octet>	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

Date	Filename	Page
22-March-2021	NZ_Govt_PKI-Schedule-A-Certificate-And-CRL-Profiles-And-Formats.Docx	47 of 47
	DMS Reference: 4631155DA	