New Zealand Government PKI  
Core Obligations Policy

|  |  |
| --- | --- |
| Date approved |  |
| Review date |  |
| Policy owner |  |
| DMS number |  |

Summary

This policy sets out the core obligations and participant requirements in relation to the application, generation, issuance and on-going management of digital keys and certificates issued for the NZ Government PKI.

Contents

[Policy Overview 2](#_Toc450294957)

[Application 2](#_Toc450294958)

[Delegated Authorities 2](#_Toc450294959)

[Definitions 2](#_Toc450294960)

[Policy detail 3](#_Toc450294961)

[Related documents 11](#_Toc450294962)

[Appendix A – Levels of Identity Proofing 12](#_Toc450294963)

[Appendix B – Certificate Profiles 14](#_Toc450294964)

[Root Certificates 14](#_Toc450294965)

[Subordinate Certificates 17](#_Toc450294966)

[Subscriber Certificate 19](#_Toc450294967)

[Appendix C – Cryptographic Standards 22](#_Toc450294968)

[Hash Function 22](#_Toc450294969)

[Asymmetric Encryption Key Algorithms 22](#_Toc450294970)

[Symmetric Encryption Algorithms 22](#_Toc450294971)

[Cryptographic Standards Reference Sources 23](#_Toc450294972)

[Appendix D – Disclaimer 25](#_Toc450294973)

[Framework Accreditation Disclaimer 25](#_Toc450294974)

# Policy Overview

## Application

1. This policy is to be read in conjunction with the New Zealand (NZ) Government Public Key Infrastructure Framework (PKIF), referred herewith in this policy as ‘the Framework’.
2. This policy applies to:
   1. New Zealand All of Government (AoG) Telecommunications as a Service (TaaS) Service Providers participating in the Framework;
   2. Non-TaaS Service Providers looking to participate in the Framework;
      1. Non-TaaS service providers wishing to participate in the Framework should contact the TaaS Lead Agency to discuss their specific requirements and solution.
      2. Non-TaaS service providers should expect to comply with the obligations set out in this policy, as well as additional assurance requirements equivalent to those of the NZ Government ICT Common Capability service providers.
   3. Agencies looking to participate in the Framework.
      1. Agencies wishing to participate in the Framework should contact the TaaS Lead Agency to discuss their specific requirements and solution.

## Delegated Authorities

1. The delegated authorities that apply are
2. The Telecommunications as a Service (TaaS) Lead Agency will not grant security Accreditation[[1]](#footnote-1) to a Service Provider that seeks through its documentation to avoid or exclude liability for breaches of its Core Obligations as specified in this policy.

## Definitions

1. The following definitions apply when interpreting this policy:

* **NZ PKI Framework (NZ PKIF)** – the framework of policies, obligations, structure, governance, operation and standards that describe the totality and boundaries of the New Zealand Government Public Key Infrastructure and associated Framework (NZ Govt PKIF). Referred henceforth in this policy as ‘the Framework’.
* **Telecommunications as a Service (TaaS) Service Providers** – TaaS Service Providers are those that have entered into a Lead Agency Agreement (a Government ICT Common Capability (ICT-CC) agreement) for the purchase of the “Authentication – PKI Services” service within the cross-government telecommunications and managed security services (TaaS).
* **Liability** – Liability is the legal obligation to compensate another party when an obligation has been breached. The source of the obligation can be a contract, a common law obligation, a statutory obligation or an equitable obligation. Liability will follow when an obligation of the kind that is spelt out in this policy is breached.

## Web Publishing Points

1. The web publishing and certificate distribution points are specified in the PKI Framework Guide.

* Certs: http://[cert.pki.govt.nz/pki/Certificates/<CAName>.crt](http://www.pki.govt.nz/certs/%3ccertname%3e.crt)
* Policies: https://[www.pki.govt.nz/policy/<policyname>.html](http://www.pki.govt.nz/policy/%3cpolicyname%3e.html)
* CRL: [http://crl.pki.govt.nz/crl/<CAName>.crl](https://crl.pki.govt.nz/crl/%3cCAName%3e.crl)
* OCSP: [http://ocsp.pki.govt.nz/](https://ocsp.pki.govt.nz/)
* LDAP: dir.pki.govt.nz



# Policy detail

General Service Provider Obligations

TaaS Service Providers MUST:

1. Meet all relevant evaluation requirements as set out in this Framework, including undertaking an assessment of all PKI-related systems following the ICT Shared Capability Security Certification Process Guidance using appropriate independent ICT-CC Security and Related Services (SRS) Panel resources.
2. Undertake a NZ Government Privacy Impact Assessment (PIA) for all PKI-related systems that collect, process, store or disclose personal information;
3. Be physically located within New Zealand and provide services from within New Zealand;
4. Employ staff able to achieve NZ Government appropriate security clearance in the establishment and management of PKI services;
5. Develop, maintain and provide PKI services in accordance with their Approved Documents;
6. Deliver and manage government PKI services over trusted networks, primarily using GNet (through TaaS), or equivalent that meets NZISM RESTRICTED protection requirements. Further details regarding protection of management traffic is below.
7. Document their compliance with the Core Obligations in their legal documentation such as Certificate Policy (CP), Certificate Practice Statement (CPS), Subscriber and Relying Party Agreements (where relevant), or into other Approved Documents submitted for approval by the TaaS Lead Agency;
8. Comply with the Accreditation and documentation requirements of this Framework; and
9. Perform an annual Compliance Audit and report findings to TaaS Lead Agency, in order to maintain NZ Government Accreditation.

Certificate Authority Obligations

|  |
| --- |
| Standards |
| A Certificate Authority (CA) under the Framework MUST: |
| 1. Ensure all digital certificates conform to the Request for Comment (RFC) 5280 (RFC-5280) format; |
| * 1. Appendix B lists the Root CA, Subordinate CA and Subscriber Certificate Profiles to be used; |
| * 1. Any digital certificate extensions that do not conform to RFC-5280 SHOULD be marked non critical; and |
| * 1. Digital certificate extensions used to issue special purpose certificates SHOULD be marked critical and only used within the defined context. |
| 1. Ensure all Certificate Revocation Lists (CRLs) conform to the X.509 v2 profiles as described in RFC-5280; |
| 1. Ensure all Online Certificate Status Protocol (OCSP) responses conform to RFC-6960 (where OCSP is supported); |
| 1. Ensure all CPS and CPs conform to the document framework as described in RFC-3647; and |
| 1. A CA SHOULD ensure all OCSP responses conform to RFC-5019. |
| **Certification Practice Statement / Certificate Profile** |
| A CA under the Framework MUST: |
| 1. Perform digital certificate lifecycle operations in a manner which is compliant with its CPS; |
| 1. Display the Framework Accreditation Disclaimer (Appendix C) in their CPS and CPs; |
| 1. Ensure the security objectives identified in the Lead Agency Risk Assessment and the objectives identified in the Framework are reflected in the CPS and CPs; |
| 1. Ensure the CP under which each digital certificate is issued clearly specifies the Key Usage within the Certificate Profile; |
| 1. Ensure all CPS and CPs undergo a legal evaluation by an authorised legal assessor from the TaaS Lead Agency; and |
| 1. Make available as much of its published CPS and CPs as necessary to allow a relying party to make an informed decision on trust. |
| A CA under the Framework MUST NOT: |
| 1. Escrow or backup Subscriber private keys used for non-repudiation; and |
| 1. Mark the Key Usage Extension in Subscriber digital certificates as both ‘critical’ and ‘mandatory’. |

|  |
| --- |
| Staff and Training |
| A CA under the Framework MUST: |
| 1. Provide all personnel performing information verification duties with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures ( including the CPS and CA CP), and PKI system management procedures (such as relevant operations manuals); |
| 1. Maintain records of such training and ensure that personnel maintain a skill level that enables them to perform such duties satisfactorily; |
| 1. Ensure staff involved in delivery of CA services maintain NZ Government security clearances and checks[[2]](#footnote-2), equivalent to at least the level stated in associated CP/CPS, or RESTRICTED if not specified; and |
| 1. Ensure staff operating a CA at a particular level of assurance have been identified to a higher level of identity proofing (e.g a CA operating at LoA 2 would require staff identified to LoIP 3). |

|  |
| --- |
| Certificate Generation |
| When generating a Digital Certificate, a CA under the Framework MUST: |
| 1. Ensure that the certificate information provided to it by a Registration Authority (RA) has been accurately transcribed into the digital certificate; |
| 1. Ensure that all other certificate information it generates itself is accurate; and |
| 1. Ensure that the digital certificate contains all the elements required by the Certificate Profile contained in the CP. |
| **Key Generation** |
| A CA under the Framework MUST: |
| 1. Ensure that keys are generated in accordance with the Framework Key Generation Ceremony Plan held in a suitable facility; and |
| 1. Ensure that each key pair to be used with a certificate can work. |
| **Possession of Private Key** |
| A CA under the Framework MUST: |
| 1. Take all reasonable actions to ensure that the Subscriber is in safe control of the activation data and private key(s) corresponding to the public key identified in the digital certificate before the private key can be used. |
| **Private Key Use** |
| A CA under the Framework MUST NOT: |
| 1. allow Root CA Private Keys to be used to sign certificates, except for the following cases:    * Self-signed certificates to represent the Root CA itself;    * Certificates for Policy and Issuing CAs (and Cross Certificates);    * Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA non-production environment certificates, and OCSP certificates); and    * Certificates issued solely for the purpose of testing products with certificates issued by the Root CA. |
| **Certificate Repository** |
| A CA under the Framework MUST: |
| 1. Generate, maintain and make available a list of revoked digital certificates[[3]](#footnote-3) in a manner accessible by all potential Relying Parties using standard protocols and technologies to enable them to verify, in a timely manner, the currency of a particular digital certificate; |
| 1. Operate and maintain its CRL and, if supported, OCSP capabilities with resources sufficient to provide a response time of ten seconds or less under normal operating conditions; and |
| 1. Ensure the location where certificates and CRLs are published has controlled and auditable write access, so that only valid certificates and CRLs issued by approved PKI entities can be published by an authorised person or process. |
| **Certificate Revocation** |
| A CA under the Framework MUST: |
| 1. Provide a process for Subscribers to request routine revocation of their own certificates. The process MUST be described in the CPS and relevant CP; |
| 1. Provide Subscribers and Relying Parties with clear process for reporting suspected Private Key compromise, certificate misuse, or other types of fraud or inappropriate conduct relating to certificates. The CA MUST publically disclose the instructions through a readily accessible online means accessible by Subscribers and Relying Parties; |
| 1. Ensure the prompt revocation of a digital certificate in accordance with the requirements of the CP under which it was issued and in accordance with the requirements outlined in the CA Requirements section for the specific accreditation Level of Assurance; and |
| 1. Revoke a certificate if one or more of the following occurs:    * The Subscriber notifies the CA that the original certificate request was not authorised and does not retrospectively grant authorisation;    * The PKIF Lead Agency or Subscriber notifies the CA that a problem with a subscribing agencies certificate(s) and/or key(s) has been reported by an authorised body (eg. NCSC, NZ-CERT);    * The CA obtains evidence that the Subscriber’s private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements outlined in the CP or CPS;    * The CA obtains credible evidence any certificate it has issued has been mishandled or misused;    * The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or other contractual or terms of use agreements that apply;    * The CA is made aware that the certificate was not issued in accordance with its CP or CPS;    * The CA determines that any of the information appearing in the certificate is inaccurate or misleading;    * The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate; and    * The CA obtains credible evidence of a possible compromise of a Subordinate CA’s private key. |
| **Key Archive and Recovery** |
| A Key Archive operated by a CA under the Framework MUST: |
| 1. Be protected commensurate with the protection afforded to the CA and MUST implement network filtering, identity segmentation and security controls corresponding to the CAs LOA; |
| 1. Ensure all private keys within the Key Archive Store are encrypted to mitigate attacks where the store is stolen and accessed offline; |
| 1. Log, audit and alert any instance of key recovery, so it can be reviewed by the appropriate authority; |
| 1. Only archive encryption keys to enable recovery of encrypted data. Keys used for digital signature or authentication MUST NOT be archived. |
| **Certificate Authority Termination** |
| In the event that a Framework accredited CA terminates its operations, whether voluntary or involuntary, the CA MUST NOT: |
| 1. Enter into any new contracts with customers, or renew existing contracts; or |
| 1. Enter into any new Subscriber Agreements, or renew existing Subscriber Agreements. |
| In the event that a Framework accredited CA terminates its operations, whether voluntary or involuntary, the CA MUST: |
| 1. Make arrangements to novate existing PKI services to another Framework accredited CA, or terminate all Subscriber agreements that were entered into in accordance with the relevant CP; |
| 1. Give notice to the TaaS Lead Agency and all associated parties (e.g. Subscribers, Relying Parties) advising them of its intention to terminate its contracts with them. The termination to be effective in accordance with the terms of the TaaS contract; |
| 1. Continue to provide the services, in particular the maintenance of a CRL or other listing of revoked digital certificates, in accordance with the contractual arrangements it has with agencies, and any relevant Approved Documents that include arrangements to accommodate significant interruptions in the provision of the service, until new arrangements have been put in place by alternative service provider(s); and |
| 1. Co-operate with the TaaS Lead Agency and other Service Providers, to achieve a seamless and secure migration of the agencies and Subscribers to an alternative Framework accredited CA. |
| **Logging** |
| The CA MUST record at least the following events: |
| 1. CA key lifecycle management events, including:    * Key generation, backup, storage, recovery, archival and destruction; and,    * Cryptographic device lifecycle management events. |
| 1. CA and Subscriber certificate lifecycle management events, including:    * Certificate requests, renewal requests, re key requests, revocation requests and revocation actions;    * Acceptance and rejection of certificate requests; and,    * Issuance of certificates. |
| 1. Generation of CRLs and if supported, OCSP entries; |
| 1. Security events, including:    * Successful and unsuccessful PKI system access attempts;    * Successful and unsuccessful PKI system denial of service, or other cyber attack attempts;    * Changes to rights assigned to PKI services privileged accounts, or associated infrastructure system administrator accounts;    * System outages, hardware failures and other anomalies;    * Firewall and router activities;    * All PKI service reports issued by NCSC or NZ-CERT and associated actions; and,    * Entries to and exits from the CA facility. |
| 1. Logs MUST be retained for a minimum of seven years after action is completed[[4]](#footnote-4). |

Registration Authority Obligations

|  |
| --- |
| Identity Proofing |
| A Registration Authority (RA) under the Framework MUST: |
| 1. Take all reasonable actions to verify the accuracy and sufficiency of recipients identity documentation, including any client application forms and supporting documentation received; |
| 1. Ensure the accurate recording and secure transmission of all relevant certificate information to the relevant CA; |
| 1. Ensure the secure storage of all retained Applicant and Subscriber information in accordance with the requirements of its Approved Documents; and |
| 1. In the event that an error is identified in the identity proofing process that gives rise to uncertainty as to the identity of a particular Subscriber, promptly notify the CA that generates the digital certificate of the error and request the revocation of the digital certificate. |
| **Levels of Identity Proofing** |
| A Registration Authority (RA) under the Framework MUST: |
| 1. Ensure the characteristics and minimum criteria for identity proofing set out in Appendix A are met at the appropriate level before asserting an identity at that level; |
| **Staff Training** |
| A Registration Authority (RA) under the Framework MUST: |
| 1. Provide all personnel performing identity verification duties with skills-training that covers basic PKI knowledge, authentication and vetting policies and procedures (including CPS and CA CP), and PKI system management procedures (such as RA Operations Manual). |
| 1. Ensure staff involved in delivery of CA services maintain NZ Government security clearances and checks[[5]](#footnote-5), equivalent to the level stated in associated CP/CPS; or IN-CONFIDENCE if not otherwise specified. |
| **RA Termination** |
| In the event that a Framework Accredited RA terminates its services, whether voluntary or involuntary, it MUST NOT: |
| 1. Conduct any new registration activities for Applicants or Subscribers. |
| In the event that a Framework Accredited RA terminates its services, whether voluntary or involuntary, it MUST: |
| 1. Give notice to the TaaS Lead Agency and all CAs with whom it has a relationship in accordance with the terms of the TaaS contract. |

Subscriber Obligations

|  |
| --- |
| General Provisions |
| A Subscriber under the Framework MUST: |
| 1. Ensure that all information provided, and any representations made to a Framework Accredited RA are complete and accurate; |
| 1. Perform any additional requirements as specified in the CP under which the digital certificate was issued; |
| 1. Take all reasonable measures to protect their private key and activation data from compromise and take all necessary precautions to prevent loss, disclosure, modification or unauthorised use of their private key; |
| 1. Promptly notify the relevant CA in the event that they consider or suspect there has been a compromise of their private key; and |
| 1. Promptly notify the relevant RA in the event that they consider the identity information provided by them is or may be incorrect. |

Relying Party Obligations

|  |
| --- |
| General Provisions |
| A Relying Party under the Framework SHOULD: |
| 1. Verify that the digital certificate is current and has not been revoked or suspended, in a manner specified in the CPS and CP under which the digital certificate was issued; |
| 1. Verify that the digital certificate is being used within the limits specified in the CPS and CP under which the digital certificate was issued; and |
| 1. Promptly notify the relevant CA in the event that they consider or suspect there has been a compromise of a Subscriber’s private key. |

# Related documents

1. The following documents are relevant to this policy:

|  |  |
| --- | --- |
| Reference | Description |
| [ACP185] | Public Key Infrastructures (PKI) Cross-Certification Between Combined Communications-Electronics Board (CCEB) Nations (http://jcs.dtic.mil/j6/cceb/acps/acp185/ACP185.pdf) |
| [ICT-SCSCPG] | The Department of Internal Affairs’ ICT Shared Capability Security Certification Process Guidance |
| [NZISM] | New Zealand Information Security Manual (http://www.gcsb.govt.nz/publications/the-nz-information-security-manual/) |
| [PRA2005] | New Zealand Public Records Act 2005 |
| [Priv2013] | New Zealand Privacy Act 1993; incorporating the Privacy Amendment Act 2011 and Privacy Amendment Act 2013 |
| [PSR] | New Zealand Government Protective Security Requirements (https://www.protectivesecurity.govt.nz/) |
| [RFC3647] | IETF Request for Comments 3647: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework |
| [RFC5019] | IETF Request for Comments 5019: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments |
| [RFC5280] | IETF Request for Comments 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| [RFC6960] | IETF Request for Comments 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP |
| [WebTrust] | AICPA/CICA WebTrust Program for Certification Authorities Version v2.0. |
| [WebTrust Audit Criteria] | WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria, V1.1, Jan 2013 |
| [EAAF] | ISO/IEC 29115:2011, Entity Authentication Assurance Framework (EAAF) |
| [EoI] | ISO/IEC 29003:DRAFT - Evidence of Identity (EoI) |

1. – Levels of Identity Proofing

#### Levels of Identity Proofing

This section (and the subsequent table) details the assurance requirements to be met by RAs. Each level defines characteristics and minimum criteria that MUST be met in order to gain and maintain accreditation at a particular level.

**LoIP 1 – Low Confidence**

At this level identity is unique within the intended context. There is little confidence in the accuracy or legitimacy of the claimed identity. Self-claimed or self-asserted identity (including pseudonymity) is possible but not anonymity.

Identity assertions at this level are appropriate for transactions with minimal consequences to Relying Parties from the registration of a fraudulent identity.

**LoIP 2 – Moderate Confidence**

At this level identity is unique within the intended context, identity has been asserted by some authoritative or corroborative sources and the Subscriber has some link to the identity. There is moderate confidence in the claimed identity.

Identity assertions at this level are appropriate for transactions with some minor consequences associated with the registration of fraudulent identity.

**LoIP 3 – High Confidence**

At this level identity is unique within the intended context, the identity is recognised by authoritative sources, identity information is verified with authoritative sources through strong processes and the Subscriber is linked to the identity. There is high confidence in the claimed identity.

Identity assertions at this level are appropriate for transactions with serious consequences associated with registration of fraudulent identity.

| Requirement | LoIP 1 | LoIP 2 | LoIP 3 |
| --- | --- | --- | --- |
| **Identity Verification** | | | |
| **Objective 1**: Identity is unique | Records within the context shall be checked for a duplicate entry. | | |
| **Objective 2**: Identity exists | Not checked | Proofing party shall get evidence that the identifying attributes exist in corroborative source(s) | Proofing party shall get evidence that the identifying attributes exist in authoritative source(s) |
| **Objective 3**: Identity is bound to a person | Not checked | The proofing party shall check binding to the identity using one of the following factors:  Something known by the subject that is not public information or reasonably accessible on the evidence of identity;  **or**  Something the subject is. | The proofing party shall check binding to the identity using two or more of the following factors:  Something known by the subject that is not public information or reasonably accessible on the evidence of identity;  **and/or**  Something possessed by the subject;  **and/or**  Something the subject is. |
| **Objective 4**: Identity’s status | Not checked | Proofing information should be verified against an authoritative source recording death. | Proofing information should be verified against an authoritative source recording death. |

The overall LoIP is determined by the minimum LoIP achieved for each objective.

1. – Certificate Profiles

The tables below contain specific certificate information and extensions to ensure operational integrity. The tables do not address all certificate extensions. Other use extensions SHOULD conform to [RFC5280]. Extensions that do not confirm to [RFC5280] SHOULD be marked non-critical. The table uses the following terms:

• **Required critical** – the extension shall be present and is always marked critical.

• **Required** – the extension shall be present and may be marked non-critical.

• **Optional** – the extension may be included at a Service Provider’s discretion.

• **Not Used** – the extension shall never be used.

Values in these tables have been based on the requirements outlined in the “Public Key Infrastructures (PKI) Cross-Certification Between Combined Communications-Electronics Board (CCEB) Nations” [ACP185].

## Root Certificates

| **F**i**e**l**d**/ **E**x**ten**sion | Root CA Certificate |
| --- | --- |
| Version | **Required** |
| V3 (2) |
| Serial Number | **Required** |
| Must be unique to an Issuer |
| Issuer Signature Algorithm[[6]](#footnote-6) | **Required** |
| * **sha256WithRSAEncryption {1 2 840 113549 1 1 11}**   Or   * **ecdsa-with-SHA384 {1 2 840 10045 4 3 3}** |
| Issuer Distinguished Name | **Required** |
| Each RDN is a printableString and contains a single attribute type and attribute value tuple |
| Validity Period | **Required** |
| Maximum 10 years from date of issue in UTC format.  Note: the notBefore component will be the certificate’s issue date. The notAfter component is the day ending the validity period. |
| Subject Distinguished Name | **Required** |
| Each RDN is a printableString and contains a single attribute type and attribute value tuple |
| Subject Public Key Information | **Required** |
| Key size to provide at least 128 bits of security strength or greater for certificates with a maximum validity period of 5 years.  The following encryption algorithms are acceptable:   * RsaEncryption {1 2 840 113549 1 1 1 } * Id-ecPublicKey {1 2 840 10045 2 1} |
| Issuer Unique Identifier | **Not Used** |
| Subject Unique Identifier | **Not Used** |
| Issuer’s Signature | **Required** |
| ASN.1 DER encoded certificate signature value corresponding to  Issuer signature algorithm |
| Authority Key Identifier | **Optional** |
| keyID, Octet String  Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| **Not Used** |
| Issuer DN, Serial Number tuple |
| Subject Key Identifier | **Required** |
| Recommended that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| Key Usage | **Required**  **Critical** |
| keyCertSign, CRLSign |
| Basic Constraints | **Required**  **Critical** |
| cA True; path length constraint absent or value per PKI hierarchy |
| Extended Key Usage | **Not Used** |
| Private Key Usage Period | **Not Used** |
| Certificate Policies | **Required** |
| Sequence of one or more policy information terms, each of which consists of an object identifier OID and optionally id-qt-cps | id- qt-unotice qualifiers |
| **F**i**e**l**d**/ **E**x**ten**sion | Root CA Certificate |
| Policy Mappings | **Optional** |
| Sequence of one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy |
| Subject Alternative Name | **Not Used** |
| Issuer Alternative Name | **Not Used** |
| Subject Directory  Attributes | **Not Used** |
| Name Constraints | **Optional** |
| AoG Root will not include Name Constraints.  If included, it shall contain permittedSubtrees or excludedSubtrees field. Recommend that if asserted it be marked critical. |
| Policy Constraints | **Optional** |
| inhibitPolicyMapping with skipcerts=0 |
| Authority Information Access | **Required** |
| id-ad-caIssuers  Primary HTTP URI mandatory  Secondary LDAP URI  optional |
| id-ad-ocsp  Optional |
| CRL Distribution Points | **Optional** |
| Primary HTTP URI mandatory  Secondary LDAP URI optional |
| Subject Information Access | **Optional** |
| Id-ad-carepository  Primary HTTP URI mandatory if extension is present  Secondary LDAP URI optional |
| Freshest CRL | **Not Used** |
| Inhibit Any Policy | **Optional** [[7]](#footnote-7) |
| skipcerts=0 |

## Subordinate Certificates

*This certificate profile applies to Policy and Issuing Certificate Authority Certificates.*

| **F**i**e**l**d**/ **E**x**ten**sion | **Subordinate** CA certificate |
| --- | --- |
| Version | **Required** |
| V3 (2) |
| Serial Number | **Required** |
| Must be unique to an Issuer |
| Issuer Signature Algorithm | **Required** |
| * ecdsa-with-SHA384 {1 2 840 10045 4 3 3}   OR   * **sha256WithRSAEncryption {1 2 840 113549 1 1 11}** |
| Issuer Distinguished Name | **Required** |
| Each RDN is a printableString and contains a single attribute type and attribute value tuple. |
| Validity Period | **Required** |
| Maximum of 5 years from date of issue in UTC format  Note: the notBefore component will be the certificate’s issue date. The notAfter component is the day ending the validity period. |
| Subject Distinguished Name | **Required** |
| Each RDN is a printableString and contains a single attribute type and attribute value tuple. |
| Subject Public Key Information | **Required** |
| Key size to provide at least 128 bits of security strength or greater for certificates with a maximum validity period of 5 years  The following encryption algorithms are acceptable:   * RSAEncryption {1 2 840 113549 1 1 1 } * id-ecPublicKey {1 2 840 10045 2 1} |
| Issuer Unique Identifier | **Not Used** |
| Subject Unique Identifier | **Not Used** |
| Issuer’s Signature | **Required** |
| ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm. |
| Authority Key Identifier | **Required** |
| keyID, Octet String  Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| **Not Used** |
| Issuer DN, Serial Number tuple |
| Subject Key Identifier | **Required** |
| Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information. |
| Key Usage | **Required**  **Critical** |
| keyCertSign, CRLSign and, optionally, others to include digitalSignature and nonRepudiation |
| Basic Constraints | **Required**  **Critical** |
| cA True; path length constraint 1 [only allow issuing CAs directly off subCA] |
| Name Constraints | **Required**  **Critical** |
| Subordinate (Policy) CAs will include Name Constraints to limit the domains under which certificates may be issued.  Name constraints can contain permittedSubtrees and/or excludedSubtrees field. |
| Extended Key Usage | **Not Used** |
| Private Key Usage Period | **Not Used** |
| Certificate Policies | **Required** |
| Sequence of one or more policy information terms, each of which consists of an OID and optionally ID-QT-CPS and ID-QT-UNotice Qualifiers. |
| Subject Alternative Name | **Not Used** |
| Issuer Alternative Name | **Not Used** |
| Subject Directory Attributes | **Not Used** |
| Authority Information Access | **Optional** |
| id-ad-caIssuers |
| Primary HTTP URI mandatory  Secondary LDAP URI optional |
| **Required** |
| id-ad-ocsp |
| CRL Distribution Points | **Required** |
| Primary HTTP URI mandatory  Secondary LDAP URI optional |
| Subject Information Access | **Optional** |
| Id-ad-carepository  Primary HTTP URI mandatory if extension is present  Secondary LDAP URI optional |
| Freshest CRL | **Not Used** |

## Subscriber Certificate

| **F**i**e**l**d**/ **E**x**ten**sion | **Subscriber Certificate** |
| --- | --- |
| Version | **Required** |
| V3 (2) |
| Serial Number | **Required** |
| Must be unique to an Issuer |
| Issuer Signature Algorithm | **Required** |
| * sha256WithRSAEncryption {1 2 840 113549 1 1 11}   Or one of the following signature algorithms:   * ecdsa-with-SHA384 {1 2 840 10045 4 3 3} |
| Issuer Distinguished Name | **Required** |
| Each RDN is a printableString and contains a single attribute type and attribute value tuple |
| Validity Period | **Required** |
| Maximum of 2 years from date of issue in UTC format if enrolled through a manual process.  Maximum of 1 year from date of issue in UTC format if enrolled through an automatic process.  Note: the notBefore component will be the certificate’s issue date. The notAfter component is the day ending the validity period. |
| Subject Distinguished Name | **Required** |
| Each RDN is a printableString and contains a single attribute type and attribute value tuple  directoryString is encoded as printableString  cn={ Host URL | Host IP Address | Host Name } |
| Subject Public Key  Information | **Required** |
| Key size to provide at least 128 bits of security strength or greater for certificates with a maximum validity period of 2 years  The following encryption algorithms are acceptable:   * RSAEncryption {1 2 840 113549 1 1 1 } * id-ecPublicKey {1 2 840 10045 2 1} |
| Issuer Unique Identifier | **Not Used** |
| Subject Unique Identifier | **Not Used** |
| Issuer’s Signature | **Required** |
| ASN.1 DER encoded certificate signature value corresponding to  Issuer signature algorithm |
| Authority Key Identifier | **Required** |
| keyID, Octet String  Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| **Not Used** |
| Issuer DN, Serial Number tuple |
| Subject Key Identifier | **Required** |
| Recommended that that the octet string contain the 20 byte SHA–1 hash of the binary DER encoding of the subject CA’s public key information |
| Key Usage | **Required** |
|  | **Critical** |
| One or more of: digital signature, non repudiation, key encipherment, data encipherment, key agreement |
| Basic Constraints | **Not Used** |
| Extended Key Usage | **Optional** |
| Private Key Usage Period | **Not Used** |
| Certificate Policies | **Required** |
| Sequence of one or more policy information terms, each of which consists of an OID and optional qualifiers |
| Policy Mappings | **Optional** |
| Subject Alternative Name | **Optional;** Recommended RFC 822 Name and UPN |
| Issuer Alternative Name | **Not Used** |
| Subject Directory Attributes | **Optional** |
| Name Constraints | **Not Used** |
| Policy Constraints | **Not Used** |
| Authority Information Access | **Required** |
| id-ad-caIssuers  Primary HTTP URI mandatory  Secondary LDAP URI optional |
| **Optional**  id-ad-ocsp |
| CRL Distribution Points | **Required** |
| Primary HTTP URI mandatory  Secondary LDAP URI optional |
| Subject Information Access | **Not Used** |
| Freshest CRL | **Not Used** |
| Inhibit Any Policy | **Not Used** |

1. – Cryptographic Standards

Only the following cryptographic options are to be used for NZ Government PKI Services (including TaaS). The specification format is based on the SEEMail v3.1 Technical Specification[[8]](#footnote-8), though the algorithm strengths are different, but both approved by DIA (AoG EA Standards) and endorsed by GCSB.

This specification is consistent with the requirements of the NZ Information Security Manual (NZISM) v2.4 dated Nov 2015.

## Hash Functions

* The default hash function used for signing MUST be SHA-256 or better.

## Asymmetric Encryption Key Algorithms

### Elliptic Curve Cryptographic (ECC) Algorithm:

* ECDSA Elliptic Curve Cryptographic (ECC) algorithm with a key length of 256-bits and P-256 (prime moduli) curve MUST be used for new implementations (SHA-256 / ECDSA-256).
* The recommended ECC schema is:
  + Signature Algorithm: **ECDSA with SHA256**
    - NIST ASN1ObjectIdentifier: {1.2.840.10045.4.3.3}
    - Description: ECDSA with SHA-256 signature values
    - RFC: <https://www.ietf.org/rfc/rfc5753.txt>
  + Key Agreement Algorithm (Hash): **ECCDH with SHA256** (dhSinglePass-cofactorDH-sha256kdf-scheme)
    - NIST ASN1ObjectIdentifier: {1.3.132.1.14.2}
    - Description: dhSinglePass-cofactorDH-sha256kdf-scheme
    - RFC: <https://tools.ietf.org/html/rfc5753.html>

### RSA Algorithm:

* RSA-4096 MUST be used for all new implementations.
* RSA-2048 SHOULD only be supported for backwards compatibility.
* The recommended RSA schema is:
  + Signature Algorithm: **RSA with SHA256**
    - NIST ASN1ObjectIdentifier: {1.2.840.113549.1.1.11}
    - Description: RSA with SHA-256 signature values
    - RFC: <https://www.ietf.org/rfc/rfc5753.txt>
  + Key Agreement Algorithm (Hash): **RSA with SHA256** (sha256WithRSAEncryption)
    - NIST ASN1ObjectIdentifier: 1.3.132.1.14.2
    - Description: dhSinglePass-cofactorDH-sha256kdf-scheme
    - RFC: <https://tools.ietf.org/html/rfc5753.html>

## Symmetric Encryption Algorithms

* AES-256 MUST be used for new implementations.
* AES-256 MUST be used for backwards compatibility (eg. Legacy agency business systems).
* AES-256 MUST NOT be used in any circumstances.
* Triple-DES MUST NOT be used in any circumstances.
* *Key Encryption using AES256 WRAP MUST follow RFC 5753 when populating KeyWrapAlgorithm parameters.*
* The recommended schema is:
  + Content Encryption Algorithm: **AES256** **(with GCM)**
    - NIST ASN1ObjectIdentifier: 2.16.840.1.101.3.4.1.46
    - Description: AES256 in CTR mode with Galois MAC
    - RFC: <https://tools.ietf.org/html/rfc5084.html>
  + Key Wrap Algorithm: **AES256 WRAP**
    - NIST ASN1ObjectIdentifier: 2.16.840.1.101.3.4.1.45
    - Description: Advanced Encryption Standard (AES) Key Wrap Algorithm
    - RFC: <https://tools.ietf.org/html/rfc3394.html>

## Cryptographic Standards Reference Sources

|  |  |  |
| --- | --- | --- |
| **RFC baselines** | **Standard** | **Reference** |
| Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile | RFC-5280 primary/preferred  and RFC-6818 supported | <http://tools.ietf.org/html/rfc5280>; and <http://tools.ietf.org/html/rfc6818> |
| Message Handling - Symmetric encryption algorithm  (AES-256 MUST be used) | RFC-5751 | <http://tools.ietf.org/html/rfc5751> |
| Advanced Encryption Standard (AES) Key Wrap Algorithm | RFC-3394 | <http://tools.ietf.org/html/rfc3394.html> |
| Certificate Handling  (especially Sect 4.2; Gateways behaviour for the handling (cacheing) of incoming Certificates and CRL’s). | RFC-5750 | <http://tools.ietf.org/html/rfc5750> |
| AES256 in CTR mode with Galois MAC | RFC-5084 | <https://tools.ietf.org/html/rfc5084.html> |
| Advanced Encryption Standard (AES) Key Wrap Algorithm | RFC-3394 | <https://tools.ietf.org/html/rfc3394.html> |
| Use of Elliptic Curve Cryptography (ECC) public key algorithms in Cryptographic Message Syntax (CMS) | RFC-5753 | <https://www.ietf.org/rfc/rfc5753.txt> |
| Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)  (ie. Public key MUST be capable of ECDSA384) | RFC-4754 | <http://www.ietf.org/rfc/rfc4754.txt> |
| Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography | NIST SP800-56A-Rev2 | <http://dx.doi.org/10.6028/NIST.SP.800-56Ar2>  <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf> |

1. – Disclaimer

## Framework Accreditation Disclaimer

|  |
| --- |
| The Telecommunications as a Service (TaaS) Lead Agency is responsible for ensuring that the accreditation process is conducted with due care and in accordance with published Framework Criteria and Policies.  The TaaS Lead Agency is not liable for any errors and/or omissions in the final Approved Documents, which remain the responsibility of the accredited Service Provider.  The New Zealand Government is not responsible and cannot be held liable for any loss of any kind in relation to the use of digital keys and certificates issued by a Framework accredited Service Provider. By granting a Service Provider Framework Accreditation the TaaS Lead Agency makes no representation and gives no warranty as to the:   * Accuracy of any statements or representations made in, or suitability of, the Approved Documents of a Framework accredited Service Provider; * Accuracy of any statement or representation made in, or suitability of, the documentation of a Service Provider in a Framework recognised PKI domain; or * Standard or suitability of any services thereby provided by any Subscriber or Relying Party or application. |

1. Refer [NZISM], Section 4. [↑](#footnote-ref-1)
2. In accordance with Personnel Security Management Protocol from the [PSR] [↑](#footnote-ref-2)
3. Otherwise known as a ‘CRL’, and in accordance with the ITU-T Recommendation [X.500] and [RFC-3647] [↑](#footnote-ref-3)
4. In accordance with the [PRA2005] and [NZISM] [↑](#footnote-ref-4)
5. In accordance with Personnel Security Management Protocol from the [PSR] [↑](#footnote-ref-5)
6. Additional encryption algorithms may need to be included to support cross certification requirements between combined communications-electronics board (CCEB) nations. [↑](#footnote-ref-6)
7. This is not conformant to RFC-5280. However is required do overcome potential application compatibility issues. [↑](#footnote-ref-7)
8. Version 1.0.6, dated 18th November 2015 [↑](#footnote-ref-8)