INTERNAL AFFAIRS
Te Tari Taiwhenua

New Zealand Government

X.509
Certification Practice Statement (CPS)
for the
New Zealand Government Public Key Infrastructure (PKI)
Root and Shared Certificate Authorities

Version 1.3
11th Dec 2020

Document Management

This document is owned, approved and controlled by:	NZ Government PKI (TaaS) Lead Agency - DIA
The document owner authorises approved changes to be made to this document by:	Cogito Group

Revisions (Change History)

Version	Revision date	Change / Amendment Description	Editor
0.1	Nov 2015	Initial draft	SJ Lillywhite
0.2/0.3	Feb 2016	Open review updates and corrections	B Fardig / SJ Lillywhite
0.4/0.5/0.6	Mar 2016	Update OIDs, CA numbers, doc meta-data, updates to reflect design changes.	SJ Lillywhite / T Butler / P Cutforth
0.7/0.8	Apr/May 2016	GCIO updates for Key Ceremony and initial PKI Framework deployment. Updates from AoG (TAG) stakeholder workshop.	SJ Lillywhite PA Cutforth
0.9	Jun 2016	Open review and design change requests (DD)	R Brown / B Fardig P Cutforth
1.0	16 Sep 16	Approved by TAG, PKI Authority and SRO	A Dean / P Cutforth
1.1	Jul 20	6-month review and updates to reflect new requirements and system changes	P Cutforth / B Fardig / D Weinstock
1.2	Sep 20	Review and minor updates	B Fardig
1.3	Dec 20	Review, updated URLs and references to GCDO	A Stephen

Approvals

Position	Organisation	Name	Signature	Date
Lead Agency SRO / CISO	DIA (CSD)	Chris Webb	*{original signed}*	16/9/16
GCIO Technical Design Authority	DIA (ST)	James Collier	*{original signed}*	16/9/16
CA Operations Manager	Cogito Group	Richard Brown	*{original signed}*	16/9/16

References

See Appendix A for References.

Contents

1. INTRODUCTION

In general, a *Certification Practice Statement* (CPS) is a statement of the practices that a *Certification Authority* (CA) employs for all *certificate* lifecycle services (e.g., issuance, management, revocation, and renewal or re-keying) and provides details concerning other business, legal, and technical matters. A *Certificate Policy* (CP) is a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements.

The headings in this CPS follow the framework set out in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

A document hierarchy applies: the provisions of any applicable contract such as a *Subscriber Agreement*, *Deed of Agreement* or other relevant contract override the provisions of a CP. The provisions of a CP prevail over the provisions of this CPS to the extent of any direct inconsistency. The provisions of this CPS govern any matter on which a CP is silent. (Note: where sub titled sections of the framework provide no additional information to detail provided in a CP they have not been further extrapolated in this document.)

This section identifies and introduces the set of provisions, and indicates the types of entities and applications to which this New Zealand Government X.509 CPS applies.

1.1 Overview

The purpose of this CPS is to provide a common framework under which the New Zealand Government *Public Key Infrastructure* (PKI), *Certificate Authority* (CA) and *Registration Authority* (RA), services are provided.

As such, this CPS sets out a number of policy and operational matters related to the services, including the practices that the New Zealand Government employs in issuing, revoking and managing certificates For the Government Network (GNet) environment and other separate PKI requirements identified in the *New Zealand Government PKI Framework.*

The concept and structure of the *New Zealand Government PKI Framework* is a three tier CA model as shown in Figure 1 and described in the related overview document. This includes a description of the expected architecture for PKI Service Providers use. The New Zealand Government PKI Framework architecture complies with the respective Government Enterprise Architecture of New Zealand (GEA-NZ) reference models and taxonomies.

This CPS is to be read in conjunction with the relevant CP, which sets out the rules regarding the applicability of a certificate to a particular community and contains information about the specific structure of the relevant certificate type and assurance level. The provisions of the relevant CP prevail over the provisions of the New Zealand Government CPS to the extent of any direct inconsistency.

Only New Zealand All-of-Government (AoG) Telecommunications as a Service (TaaS) Common Capability approved vendors[1] are nominated to provide and operate PKI services on behalf of the New Zealand Government that comply with this CPS. These PKI services are to be capable of supporting multiple CAs to provide different certificate types. These approved vendors are referred to as '*Approved AoG/TaaS PKI Service Providers*' in this document.

[1] As at April 2017, the approved vendors authorised to provide AoG PKI Services as 'Approved AoG/TaaS PKI Service Providers' are Cogito Group, Datacom, and Dimension Data NZ.

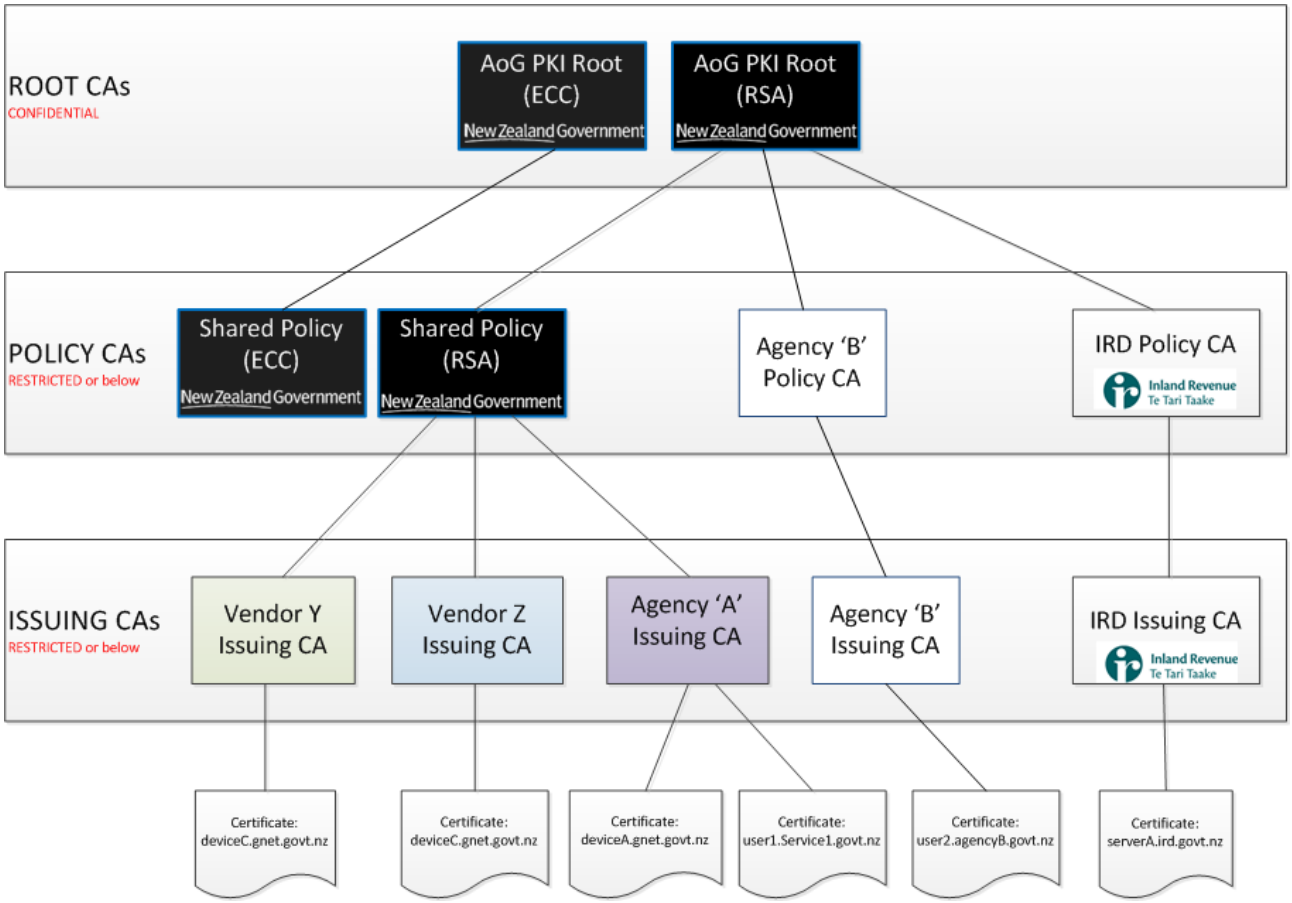


Figure 1 - NZ Government PKI Structure – Logical View

The principal governance and guiding documents referenced by this CPS are:

- the Protective Security Requirement (PSR);
- the NZ Government ICT Security Manual (NZISM);
- the New Zealand Government PKI Framework Overview; and
- the New Zealand Government PKI Framework Core Obligations policy.

The New Zealand Government PKI conducts its role in accordance with the *Approved Documents*, which are maintained by the respective Approved AoG PKI Service Providers. The baseline Approved Documents comprise:

The following public documents:

i. this CPS;
ii. the X.509 Certificate Policy for the New Zealand Government **Root Certificate Authority and Subordinate Certificate Authorities**;
iii. the X.509 Certificate Policy for the New Zealand Government **Individual – Hardware Certificates (High Assurance)**;
iv. the X.509 Certificate Policy for the New Zealand Government **Individual – Software Certificates (Medium Assurance)**;
v. the X.509 Certificate Policy for the New Zealand Government **Secure Communications Resource Certificates**;
vi. the X.509 Certificate Policy for the New Zealand Government **Validation Authority Certificates;**

vii. the New Zealand Government PKI Subscriber Agreement.

The following non-public documents:

i. New Zealand Government PKI Security Profile containing;

   a) Security Policy;
   b) System Risk Management Plan;
   c) System Security Plan; and
   d) Key Management Plan.

ii. PKI Disaster Recovery and Business Continuity Plan (PKI DRBCP);
iii. AS Operations Manual (AS Ops Man) ; and
iv. PKI Registration Authority Operations Manual (RA Manual)

Whilst the documents are named in this CPS, the contents are not disclosed publicly for security reasons.

The Approved AoG PKI Service Providers operate and manage PKI facilities on behalf of the New Zealand Government to support:

i. interaction directly with New Zealand Government Agency's assets or systems, using Public Key Technology (PKT);
ii. authentication with third parties as a subscriber of the New Zealand Government; or
iii. provision of digital signatures to entities affiliated with subscribers of the New Zealand Government PKI.

Cogito Group also provide TaaS 'Authentication Services' through the New Zealand Government PKI and use the above documentation in support of that role.

The Governance and Policy Board responsible for the New Zealand Government PKI Framework and services is the *Lead Agency*. The PKI operating at an enterprise level across the New Zealand Government provides certificate management covering:

i. identity certificates;
ii. resource certificates;
iii. PKI Infrastructure certificates (CAs, CRLs etc);
iv. application and code-signing certificates; and
v. additional certificates types as approved by the Lead Agency.

It is the responsibility of the Lead Agency to ensure that this CPS is suitable to support the certificates issued by the New Zealand Government PKI, and to approve updates to the CPS as necessary to support any additional certificates types.

Any entity within the New Zealand Government running or planning to provide a PKI service outside of this hierarchy requires approval from the Lead Agency to operate a facility for their specific application area, and this service is to be constrained to that specific applications area and not to offer a more generic service.

1.2 Document name and identification

The title for this CPS is "X.509 Certification Practice Statement for the New Zealand Government PKI".

1.3 PKI participants

1.3.1 Certification Authorities (CA)

The *Certificate Authority* (CA, or CAs), that issue certificates under this CPS are New Zealand Government CAs subordinate to a *New Zealand Government Root CA* (RCA). Appendix B provides a list of CAs operated by the Approved AoG PKI Service Providers (see Para 1.3.6) on behalf of the New Zealand Government under this CPS. Details of CAs approved by the Lead Agency to operate internally are not externally published.

1.3.2 Registration Authorities (RA)

The *Registration Authority* (RA), or RAs, that perform the registration function under this CPS are New Zealand Government RAs or New Zealand Government approved "Third Party" RAs (Authorised RAs). An RA is formally bound to perform the registration functions in accordance with the applicable CP and other relevant documentation via an appropriate agreement with the Lead Agency[2].

1.3.3 Subscriber Authorities

The *Subscriber Authority* (SA) that authorise Subscriber Certificate requests are New Zealand Government agency responsible representatives (such as CSO, CISO, ITSM or equivalent ICT management position) in respective Participating Agencies. The SA is recognised as the person or legal entity that applied for Subscriber Certificates, and / or entered into the Subscriber Agreement, in respect of that Certificate. An agency SA will be responsible for maintaining a record of all the Participating Agencies Certificates and conducting regular audits (especially to determine redundant, obsolete and retired certificates).

1.3.4 Subscribers

A Subscriber is, in the context of this overarching CPS, defined as an organisation (agency) whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant CA Certificate; or the legal entity that applied for that Certificate, and/or entered into the Subscriber Agreement in respect of that Certificate.

Note that '*Individual CPs*' provide the definition of Subscriber relevant to that CP. Typically, Individual CPs will define a Subscriber as the entity (e.g. an individual, device, web site, application or resource) whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant end Certificate; and/or the person or legal entity that applied for that Certificate, or entered into the Subscriber Agreement in respect of that Certificate.

Within the New Zealand Government PKI Framework, human Subscribers are not to request their own certificates directly from a RA. This constraint does not apply to non-human Subscribers (i.e.. machine-to-machine or device auto-enrolment certificates).

1.3.5 Relying parties

In general, a *Relying Party* uses a New Zealand Government certificate to:

i. verify the identity of an entity;
ii. verify the integrity of a communication with an entity;
iii. establish confidential communications with an entity; and
iv. ensure the non-repudiation of a communication with an entity.

In order to give uninhibited access to revocation information and subsequently invoke trust in its own services, the New Zealand Government refrains from implementing an agreement with the Relying

[2] Note that the RA's could be any one of the Approved Providers, but only the Lead Agency has responsibility to set policy.

Party with regard to controlling the validity of certificate services with the purpose of binding Relying Parties to their obligations.

Use of the New Zealand Government PKI by Relying Parties is governed by the conditions set out in the New Zealand Government PKI policy framework consisting of the Approved Documents.

Relying Parties are hereby notified that the conditions prevailing in the CPS, and relevant CP, are binding upon them when they consult the New Zealand Government PKI for the purpose of establishing trust and validating a certificate.

Relying Parties are hereby notified that no financial liability is associated with this CPS or associated CPs, or CA and RA service providers.

A Relying Party is responsible for deciding whether, and how, to establish:

i. the validity of the entity's certificate using certificate status information;
ii. any authority, or privilege, of the entity to act on behalf of the New Zealand Government;
iii. any authority, access or privilege the entity has to the Relying Party's assets or systems;
iv. any liability arising from relying on New Zealand Government PKI Framework.

A Relying Party agrees to the conditions of the relevant CP and are to:

i. verify the validity of a digital certificate i.e. verify that the digital certificate is current and has not been revoked or suspended, in the manner specified in the CP under which the digital certificate was issued;
ii. verify that the digital certificate is being used within the limits specified in the CP under which the digital certificate was issued; and
iii. promptly notify the New Zealand Government PKI in the event that it suspects that there has been a compromise of the Subscriber's Private Keys.

1.3.6 Other participants

Other participants include:

i. **Government Chief Digital Officer (GCDO)**, as the Government ICT Functional Lead, is responsible for the governance, regulation, and assurance of the New Zealand Government PKI Framework and;

   a) provides strategic direction for Public Key Technology (PKT) addressing New Zealand Government, National and International issues;
   b) owns the overarching PKI Framework approved documents;
   c) authorises establishment and connectivity of all Sub-CAs in the Government PKI and trust chain;
   d) approves agreements and requests for interoperation with other PKIs;
   e) monitors the governance and performance of the New Zealand Government PKI; and
   f) authorises establishing the PKT infrastructure to support PKI within the New Zealand Government.

ii. the **Lead Agency** – which is responsible for the delivery of the New Zealand Government PKI environment and owns the overarching policy under which this CPS operates, and:

   a) owns the All of Government Root ECC and RSA CAs;
   b) governance, performance and security accreditation matters;
   c) reviews and approve this CPS and related CPs;
   d) ensures that the infrastructure remains compliant at all times within the terms of its accreditation;
   e) presides over the PKI audit process;
   f) defines rules, and approve agreements, for interoperation with other PKIs;

g) manages the PKI Service Catalogue and commercial agreements;
h) approves mechanisms and controls for the management of the accredited PKI infrastructure (CA/RA);
i) approves operational standards and guidelines to be followed;
j) management and reporting of all CA/RA's operating under this CPS and associated CP.

iii. **Subscribing (or Accreditation) Agencies** (see also 'Subscriber Authorities')– agencies that subscribe (procure) the PKI Services are to comply with their obligations as per the PKI policy framework (Core Obligations Policy); and provide independent assurance that the facilities, practices and procedures used to issue New Zealand Government certificates comply with this CPS, related CPs, and relevant accreditation frameworks (policy, regulatory and legal) that meet their agency requirements;

iv. **Approved AoG PKI CA Service Providers** – The AoG Telecommunications as a Service (TaaS) commercial arrangements provide the mechanism to approve selected vendors as AoG PKI CA and Certificate providers. Only service providers selected under the TaaS commercial construct can provide NZ Government PKI services and certificates. Currently, the three approved service providers are Cogito Group, Datacom and Dimension Data.
Separately, Cogito Group also provide the AoG Root CA and Shared Policy CA under an extension of the TaaS arrangements (see Figure 1).

v. **Directory Service providers** – to provide a *repository* for certificates and certificate status information issued under the CP; and

vi. **System Administrators** – to act as installer for New Zealand Government PKI Resource certificates.

vii. **Authentication Service Operators** – Operate the PKI within the bounds of the accreditation frameworks.

1.4 Certificate usage

Certificates issued under this CPS, in conjunction with their associated private *keys*, allow an entity to:

i. authenticate to a Relying Party electronically in online transactions;
ii. digitally sign electronic documents, transactions, application code, timestamps and communications; and/or
iii. confidentially communicate with a Relying Party (data in transit);
iv. apply approved encryption of data in storage (data at rest);
v. issue Certificates for Root, Policy and Issuing CAs;
vi. validate certificate status through CRL signing and OCSP responses.

1.4.1 Appropriate certificate uses

See relevant CP.

1.4.2 Prohibited certificate uses

See relevant CP.

1.5 Policy administration

This section defines the administrative details for all aspects of this CPS and any applicable CPs.

1.5.1 Organisation administering the document

The Lead Agency, through the GCIO, is the authorising organisation for this CPS and applicable CPs.

Cogito Group, through the Lead Agency, is the endorsed organisation for delivering this CPS and associated Shared Policy CA CPs, including any amendments.

The Approved PKI Service Providers and Subscribing Agencies, through agreement with the Lead Agency, may also endorse this CPS as satisfying their requirements for a specific CP. The Approved PKI Service Providers are to maintain a list of organisations and certificate types for which such agreements exist.

1.5.2 Contact person

Contact details for Lead Agency:

eMail: TaaS@dia.govt.nz / gcdo@dia.govt.nz
Postal Address: Department of Internal Affairs
147 Lambton Quay
PO Box 805
Wellington 6140
New Zealand

Contact details for Cogito Group:

eMail: authentication.services@cogitogroup.co.nz
Postal Address: Cogito Group
PO Box 539
Lambton Quay
Wellington 6145
New Zealand

1.5.3 Authority determining CPS suitability for the policy

The Lead Agency is the authority responsible for determining if this CPS is suitable for a CP.

1.5.4 CPS approval procedures

This CPS is approved by the Lead Agency and endorsed by the GCDO and GCISO.

Before accepting changes to this CPS and related CPs:

i. the proposed changes are to be integrated into a draft document and submitted to the Lead Agency for review;
ii. the proposed changes are reviewed and presented to the PKI Technical Advisory Group (TAG) for endorsement; [iteration]
iii. once the proposed changes are acceptable, the Lead Agency will present the changes to the AoG CISO, through the ICT Common Capabilities Security Risk Steering Group (ICT-CC SRSG), for approval;
iv. approved changes are forwarded to external parties who perform any PKI accreditation or cross certification process with the New Zealand Government; and
v. upon acceptance by all parties, the Lead Agency will authorise the proposed changes for publication and implementation by the authorised PKI Service Providers.

1.6 Definitions, acronyms and interpretation

See Appendix C – Definitions, Acronyms and Interpretation. Note that all defined terms in this CPS appear in italics the first time they are used and otherwise are not identified in this manner when appearing later throughout the CPS.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Approved PKI Service Providers are to operate repositories supporting the New Zealand Government PKI and its operations.

On behalf of the Lead Agency, Cogito Group are to operate an external online repository that holds authoritative New Zealand Government PKI related information (such as Certificates, CRLs, formal documentation, service updates, compromise notifications, etc.) relevant to the AoG PKI services.

The external online Certificate, CP, CRL repository is to be accessible at the URI http://pki.govt.nz/.

The additional repository for this CPS, relevant CP's, PKI Disclosure Statements, related information resources, service and compromise notifications, and other NZ Government PKI collateral will be accessible at https://www.pki.govt.nz. This site will comply with AoG web standards, policies and templates.

Publicly accessible information regarding the AoG PKI, the Framework and associated TaaS services will also be available at digital.govt.nz.

2.2 Publication of certification information

Approved PKI Service Providers are to publish to their internal repository all CA certificates, relevant *Subscriber* certificates and *Certificate Revocation Lists* (CRL).

See Section 2.1 for details of external certificate publishing resources for Subscribers and Relying Parties. Subscribing Agencies are to ensure the external internet-facing web resources at pki.govt.nz are available either directly or via "proxy" repositories in their agency enterprise network.

CA Certificates, Entity Certificates and CRLs that are not required for external use or external Relying Parties, will not be published in external repositories. Resource certificates for non-person entities such as New Zealand Government applications, servers, routers and so forth may be published to a certificate store within an application as an alternative to publication within the repository.

2.3 Time or frequency of publication

The prompt publishing of information in the repository is required after such information becomes available. This CPS specifies the minimum performance standards applicable to the various types of information in Section 4 (Certificate Lifecycle Operational Requirements).

Public documents are published/updated promptly on approved change and are to be reviewed annually, if no changes have been approved in the interim.

Publication frequencies for certificates and CRLs are detailed in the applicable CP.

2.4 Access controls on repositories

Repository information requires protection from unauthorised disclosure or modification, appropriate for the classification of the information and its value to all parties.

There are no further access controls on read-only versions of public documents.

Appropriate access controls on the repositories are used to ensure that only personnel and processes authorised by the Lead Agency are able to write to, or modify repository information.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

See Relevant CP

3.1.2 Need for names to be meaningful

See relevant CP for details.

3.1.3 Anonymity or pseudonymity of Subscribers

See relevant CP.

3.1.4 Rules for interpreting various name forms

See relevant CP.

3.1.5 Uniqueness of names

See relevant CP.

3.1.6 Recognition, authentication, and role of trademarks

Applicants for certificates are to take all reasonable steps to ensure that subject names do not contain or comprise anything that might infringe a trademark.

The CA will not issue a certificate where it is aware that it would contain a name that infringes (or that the CA considers might infringe) a trademark.

Where the CA becomes aware subsequent to issuing that a name on the certificate contains or comprises anything that might infringe a trade mark (and hence has been erroneously issued), the certificate may be revoked as provided for in 4.9 of this CP.

It is not anticipated that trademarks or other intellectual property rights will exist in personal names used within Government certificates. If a Subscribing Agency's legal name is also a trademark, use of the name is authorised by virtue of the organisation's signing of the Subscriber Agreement[3] and acceptance of this CPS.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The Lead Agency endorses all methods used to prove possession by an entity or entity owner of the private key. See relevant CP for further details.

3.2.2 Authentication of organisation identity

See relevant CP.

3.2.3 Authentication of individual identity

The New Zealand Government PKI Framework acknowledges ISO/IEC DIS 29003, Evidence of Identity (EoI), as the approved Standard to apply to individual identity assertion and level of identity proofing (LoIP).

[3] In context of the AoG PKI Framework, the TaaS 'PKI Subscription Form' is the document that covers the obligations of a PKI 'Subscriber Agreement'.

Subscribers requiring certificates from this PKI will be subject to an EoI process performed by the appropriate Subscriber Authority as part of their certificate request.

See relevant CP for details.

3.2.4 Non-verified Subscriber information

See relevant CP.

3.2.5 Validation of authority

See relevant CP.

3.2.6 Criteria for interoperation

The decision to cross certify, cross recognise, mutually recognise, at the New Zealand Government level, or other form of interoperation with a third party PKI resides with the GCIO, Lead Agency and the third party.

The Lead Agency will inspect the third party CP, and the *X.509* Certificate Profiles, for compatibility and intended uses, as well as the CPS to ensure that the practice and procedures are also compatible.[4]

3.3 Identification and authentication for re-key requests

See relevant CP.

3.4 Identification and authentication for revocation requests

See relevant CP.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

The RCA, CA and RA certificates are created at a formal key generation and signing ceremony. Rather than being applied for, these certificates are commissioned as an integral step in implementing the PKI.

Applications for Subscriber certificates are currently restricted to the Public Sector and trusted partners and agents (i.e.. Those involved in agency or government-government and business-government transactions).

Individuals affiliated with the New Zealand Government or a New Zealand Government PKI subscriber can request a certificate application for either themselves or a resource (non-person entity), through the appropriate Subscriber Authority. New Zealand Government PKI subscriber affiliations are validated in the registration process.

If the relevant CP allows it, an authorised resource can submit an application for a New Zealand Government certificate.

The Lead Agency determines which types of affiliations with the New Zealand Government are appropriate for a certificate issued under the relevant CP.

[4] This does not mean 100% equivalent, but more that for the intended purposes of interoperation the third-party system and processes, are acceptable.

It is expected that in time, the New Zealand Government PKI Framework will expand to include citizen-to-government use cases, which will require a review of this CPS and addition of new CPs.

4.1.2 Enrolment process and responsibilities

The relevant CP will describe unique conditions, though the following is the overarching process for all CPs issued under the New Zealand Government PKI.

For RCA, CA and RA certificates, a formal key generation and signing ceremony is scripted prior to the event[5]. Highly trusted government staff from multiple agencies will fill participant roles (such as PKI trusted custodians and official witnesses), along with PKI operational and co-ordination staff from the PKI Service Provider who provide technical support for conducting the ceremony.

Registration for Subscribers may vary according to certificate type:

- Generally, individuals requiring keys and certificates are to submit an application in accordance with individual Agency processes through their Subscriber Authority.
- Applications are to contain information that is accurate, complete and up to date.
- Subscribers will, be bound by contract, code of conduct, or equivalent arrangement for trusted public agents and partners. This is in addition to their use being subject to the provisions of the applicable PDS, CP and this CPS.
- The agency Subscriber Authority is responsible for:
    - confirming the Subscriber's identity, ensuring the certificate request form is approved, [or];
    - confirming that the Subscriber has an existing entry in the Ministry's corporate directory, [and];
    - forwarding the certificate request to the RA Operator, and maintaining a record of the request.
- The RA Operator is responsible for ensuring the certificate application documentation is complete, and conduct internal procedures to issue the certificate (as per the RA Operations Manual).

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

See relevant CP. See section 3.2.3 for EoI requirements.

4.2.2 Approval or rejection of certificate applications

See relevant CP.

4.2.3 Time to process certificate applications

See relevant CP.

[5] A template for a Key Generation Ceremony is contained in the Framework Approved Documentation. This template outlines the process and controls expected to maintain a high assurance standard.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The RCA certificate is self-generated and self-signed. This occurs at the key signing ceremony. The RCA signs the CA certificate. Each CA includes "Master User" system accounts. These accounts are generated during the installation of the CA software and are password based. The RCA Master User accounts are used to authorise the signing of the CA certificate.

In accordance with the respective Approved PKI Service Providers Key Management Plan, the Policy and/or Issuing CA shall:

i. authenticate a certificate request, to ensure that it has come from an accredited or approved source[6];
ii. verify the request is correctly formed;
iii. perform any additional process as specified in the PKI Operations manual;
iv. compose and sign the certificate;
v. provide the certificate to the entity; and
vi. publish the certificate in accordance with this CPS and relevant CP.

The certificate issuance process provides an auditable record containing at a minimum:

i. details of the certificate request;
ii. the success, or rejection (with reason), of the certificate request; and
iii. the entity that submitted the certificate request.

The CA is not bound to issue keys and certificates to any entity despite receipt of an application.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

Notification to the Subscriber Authority and applicant occurs for a certificate request either when it succeeds or fails.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

See relevant CP.

4.4.2 Publication of the certificate by the CA

Certificates will be published to Hyper Text Transfer Protocol (HTTP) and Lightweight Directory Access Protocol (LDAP) repositories (see also Section 2). Resource certificates may be published to the relevant entity certificate store as an alternative to publication in a repository.

Individual CPs may have additional detail.

4.4.3 Notification of certificate issuance by the CA to other entities

The RCA and CA key generation and signing ceremony is an important government event and will be publicised accordingly as agreed by the Lead Agency and Subscribing Agency; through https://pki.govt.nz, https://digital.govt.nz, email distribution, GCIO newsletters, and media channels.

[6] For accredited CAs it must come from an accredited RA

4.5 Key pair and certificate usage

Use is restricted according to the terms of the Subscriber Agreement, the PDS, CP and this CPS. The applicable Subscriber Agreement and PDS will be the best indicators of permitted usage for a given certificate type.

See relevant CP for additional criteria.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

This CPS permits certificate *renewal*. Though 'renewal' is not the preferred process to issue a replacement certificate in the New Zealand Government PKI (see Section 4.7.1).

RCA and CA certificate renewal can occur only at formal key generation (renewal) ceremonies.

The minimum Lead Agency defined criteria for certificate renewals is:

i. the entity has an approved affiliation with the New Zealand Government or a New Zealand Government PKI subscriber; and
ii. the new validity period will not extend beyond the approved cryptographic life of the private keys.

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

The relevant CP may define additional criteria.

4.6.2 Who may request renewal

If renewal is permitted by the relevant CP, and the parties that may request renewal are not defined in the CP, then renewal requests may only be undertaken by the parties identified in 4.1.1 (Who can submit a certificate application).

4.6.3 Processing certificate renewal requests

See relevant CP.

4.6.4 Notification of new certificate issuance to Subscriber

See relevant CP.

4.6.5 Conduct constituting acceptance of a renewal certificate

See relevant CP.

4.6.6 Publication of the renewal certificate by the CA

See relevant CP.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

This CPS permits certificate *re-key.* Certificate re-key, rather than 'renewal', is the preferred process to issue a replacement certificate in the New Zealand Government PKI. Re-key indicates issuance of completely new keys and certificates. Where allowed by the respective CP and Section 4.3.1 of this CPS, the circumstances for certificate re-key include:

i. normal certificate expiration[7];
ii. certificate revocation[8];
iii. useable life of current key material has been reached; or
iv. change in algorithm, or key length, required.

The Lead Agency may define other circumstances that initiate certificate re-key. When these circumstances are defined they will be published in the relevant CP.

4.7.2 Who may request certification of a new public key

See relevant CP.

4.7.3 Processing certificate re-keying requests

See relevant CP.

4.7.4 Notification of new certificate issuance to Subscriber

See relevant CP.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See relevant CP.

4.7.6 Publication of the re-keyed certificate by the CA

See relevant CP.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

See relevant CP.

A modified certificate is required to maintain the same level of trust and assurance as the original issued certificate.

4.8.2 Who may request certificate modification

See relevant CP.

4.8.3 Processing certificate modification requests

See relevant CP.

4.8.4 Notification of new certificate issuance to Subscriber

See relevant CP.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.4.1 (Conduct constituting certificate acceptance).

4.8.6 Publication of the modified certificate by the CA

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

[7] Therefore the certificate cannot be 'renewed'.

[8] Includes situation where one or more of the details contained in the Certificate has changed (such as Subscribers name).

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Unless otherwise stated in the relevant CP, a certificate must be *revoked* if one of the following conditions applies:

i. upon suspected or known compromise of the private key;
ii. upon suspected or known loss or compromise of the media holding the private key;
iii. when a certificate has been issued erroneously or with incorrect content and needs to be reissued;
iv. when an entity (Subscriber) ceases to be employed or function within the terms and conditions of the original certificate request (e.g. Subscriber is dismissed or moves departments/);
v. when an entity fails to comply with obligations set out in the CPS, the relevant CP, or any other agreement or applicable law; or
vi. if the New Zealand Government PKI Framework or associated services are terminated

RCA, CA and RA certificates are to be immediately revoked under any of the above conditions.

Revocation would also occur in the event of PKI termination.

Expiry of a certificate shall not require revocation of the certificate.

A revoked certificate must be included on all new publications of the CRL until the certificate expires.

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

4.9.2 Who can request revocation

Revocation of the RCA or CA certificates due to a business decision to terminate the PKI would be a significant AoG event, requiring formal consultation, documentation and contingency planning. This would be managed by the Lead Agency.

Certificate revocation requests may be submitted by any of the following authorised parties:

i. Lead Agency;
ii. Subscriber Authority (on behalf of the Subscribing Agency)[9];
iii. Subscriber Agency CSO, CISO or ITSM[10];
iv. an AS Operator (for PKI core components), RO; or
v. the Subscriber[11].

4.9.3 Procedure for revocation request

The procedure for revoking certificates is set out in the relevant CP. The revocation process that applies will depend on the type of certificate being revoked.

4.9.4 Revocation request grace period

It is expected that once initiated, the revocation process is to be completed.

[9] Subscriber's direct or indirect manager must request revocation through the agency Subscriber Authority.

[10] Where they are not the Subscriber Authority, but the RA is not able to contact the Subscriber Authority for authorisations process.

[11] only in an emergency (such as a compromise), a Subscriber may request revocation directly through the RA, but their respective Subscriber Authority must be informed immediately upon revocation.

See relevant CP for additional criteria.

4.9.5 Time within which CA must process the revocation request

RCA, CA and RA certificates are to be immediately revoked, normally expected to be within 24 hours of a confirmed incident/compromise.

See relevant CP for additional criteria.

4.9.6 Revocation checking requirement for Relying Parties

It is the Relying Parties responsibility to determine their requirement for revocation checking.

4.9.7 CRL issuance frequency (if applicable)

See relevant CP.

4.9.8 Maximum latency for CRLs

All New Zealand Government repositories responsible for providing CRLs to Relying Parties shall be updated within the time frame specified in the CP, and in no case should this exceed 6 months.

The latency time in each CP is to account for the time required to:

i. generate the CRL;
ii. transfer the CRL from the CA to the master repository;
iii. replicate the master repository to subordinate repositories; and
iv. scheduled periods of system unavailability.

4.9.9 On-line revocation/status checking availability

Online Certificate Status Protocol service (*OCSP*) is available for some certificate types; refer to the relevant CP.

The latest CRL is available from the published repositories; refer to 8.1 (Repositories) and the certificate's CRL Distribution Point in the respective CP for further information.

4.9.10 On-line revocation checking requirements

See relevant CP, otherwise no stipulation.

4.9.11 Other forms of revocation advertisements available

In the event of the need to revoke a CA certificate, if the CA is involved in any form of external recognition arrangement, the relevant external parties are to be informed using the mechanisms identified in the arrangement.

Agency Subscriber Authority is to be notified in all cases of Subscriber certificate revocation.

Lead Agency is to be notified, and in most cases will have been consulted, in all cases of CA certificate revocation.

4.9.12 Special requirements re key compromise

Any compromise of private keys or RCA, CA certificates are to be reported to the Lead Agency and the National Cyber Security Centre (NCSC)[12] within 24 hours of the incident, or in accordance with the Incident Management Plan where different.

See relevant CP for additional criteria.

[12] http://www.ncsc.govt.nz/incidents/

4.9.13 Circumstances for suspension

See relevant CP.

4.9.14 Who can request suspension

See relevant CP.

4.9.15 Procedure for suspension request

See relevant CP.

4.9.16 Limits on suspension period

See relevant CP.

4.10 Certificate status services

4.10.1 Operational characteristics

The Lead Agency shall arrange to store and make available via an *internal* (cross-agency Intranet with access-controls in place[13]) web site:

i. the RCA and Sub-CA certificates;
ii. all valid individual (human) and applicable resource (non-person) certificates and cross-certificates; and
iii. the most up-to-date CRL(s).

The Lead Agency will publish relevant New Zealand Government PKI information for Relying Parties and agency consumption *externally* (via publicly accessible Internet websites at www.pki.govt.nz and www.ict.govt.nz). The CP will define what information is provided.

Once a certificate has been revoked, the CA will write the certificate serial number to the CRL, which is published periodically to the New Zealand Government repository. While Subscriber certificates are revoked immediately after the CA processes the revocation request, any end user checking the validity of a certificate will not be able to detect the revocation until the next CRL posting or their application requires a new CRL. The details of CRL publishing frequency is documented in the CP of the issuing CA.

Revocation of a CA certificate will require an immediate out-of-sequence CRL publication. Such CRL releases will be notified to the Lead Agency, other Government PKI Service Providers[14], and affected agency Subscriber Authorities immediately and out-of-band (e.g. via email distribution list; telephone contact list).

Information exchanged between the CA and the Validation Authority shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued.

4.10.2 Service availability

Cogito Group on behalf of the New Zealand Government shall make the associated services available continuously, except for unavoidable activities. Due to the nature of the Internet and internal New Zealand Government communications this service cannot be guaranteed to be always accessible.

This CPS and associated PKI core services are to be available during the New Zealand Time Zone business hours of 8am to 5pm, Monday to Friday; excluding New Zealand Public and Statutory

[13] This could be through Common Web Platform (CWP), Public Sector Intranet (PSI) or equivalent protected facility.

[14] For mitigating actions from impact on the whole Government PKI Framework trust chain.

Holidays. Monitoring and incident reporting of the PKI services is to occur continuously outside these hours.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

A subscription for a certificate ends:

i. when a certificate is revoked or allowed to expire; or
ii. when all tokens containing the certificates matching private key have been surrendered to an RA and destroyed or zeroised in an approved manner; or
iii. when the PKI is terminated.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Key escrow and recovery is supported when dual *key pairs* and certificates are issued, one for authentication and one for confidentiality. Key escrow is permitted for end entity confidentiality private keys but not for end entity signature/authentication private keys.

Recovery of end entity confidentiality keys is overseen by personnel in a PKI *Trusted Role*.

Key escrow and recovery is used to support certificate renewal/re-key/modification functions where they are authorised by the CP. In addition, the CA may, as required by law or authorised by New Zealand Government officials, recover the entities private confidentiality key and decrypt any data encrypted with the corresponding *public key*.

Authorised Key Retrievers (AKRs) are either:

i. Subscriber Authorities;
ii. a RO who may request key retrieval on behalf of a Subscriber; or
iii. Authorised government officials where criminal or national security matters are involved.

Escrow and backup of PKI *core component* keys is permitted to facilitate key recovery in a disaster recovery situation. However, cloning of *hard tokens* is not permitted.

The Lead Agency is to approve any process that provides for the escrow, back-up or archiving and subsequent recovery of private keys, see also 6.2.3 (Private key escrow). Documentation of these processes is summarised in the CP.

For the RCA, a **minimum** of three personnel are required to authorise and conduct any instance of private key recovery (two operators to conduct technical key recovery; and one government person to authorise and monitor operations) involving the RCA.

In most circumstances, Subordinate CAs will also require a minimum of two authorised technical personnel and a govt/agency assurance person.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

All New Zealand Government approved PKI Facilities[15] are located, constructed and controlled in accordance with New Zealand Government PSR and NZISM requirements for RESTRICTED protection. Approved government data centre facilities[16] are to be used whenever possible.

Section 8 details the responsibilities for Certification and Accreditation (C&A) of PKI facilities.

All PKI facilities (CAs, RAs, and distributed RAO workstations) are to be operated in suitably controlled environments.

Approved PKI Service Providers are responsible for the physical protection of PKI assets, though it is expected this will be as per the data centre facility providers arrangements. PKI components are to be protected to the same standards as other IT hardware assets serving government agencies.

5.1.1 Site location and construction

See Section 5.1.

5.1.2 Physical access

See Section 5.1.

Access to New Zealand Government PKI Facilities is to be restricted to authorised people, and all access monitored and logged.

Data centre facility staff are not to have access to New Zealand Government PKI assets at any time.

5.1.3 Power and air conditioning

See Section 5.1.

5.1.4 Water exposures

See Section 5.1.

5.1.5 Fire prevention and protection

See Section 5.1.

5.1.6 Media storage

All PKI media is stored in accordance with New Zealand Government PSR for the "Security Classification" of the information stored on the media, as stated in respective CP.

Private keys or other PKI controlled information is not to be stored or temporarily written to unprotected (unencrypted) media, including portable storage devices.

HSMs are to be used to secure the RCA and CA private keys in order to mitigate physical environment control requirements.

5.1.7 Waste disposal

Disposal of classified waste is to be in accordance with the PSR.

[15] Approved PKI Service Providers are to provide a resilient disaster recovery architecture, typically through geo-dispersed dual-facility arrangements (eg. Primary and secondary/backup operating centres). All PKI Facilities, such as primary and backup operating centres, and remote management and control centres, must comply with these CPS requirements.

[16] Such as the AoG IaaS environments.

5.1.8 Disaster recovery site

All PKI RCA and CA core components are to be available in dual-site mode, with both sites operating to the same security standards and being geographically dispersed. The secondary or backup site may be offline, but with a restoration/activation period of no more than 3 working days.

It is expected that all New Zealand Government PKI CA facilities and assets will be equally treated and provisioned as the RCA and core components.

See also Section 5.1.

5.2 Procedural controls

5.2.1 Trusted roles

This CPS identifies which roles are "*Trusted Roles*". Personnel occupying trusted roles will require security clearances in accordance with policy for IT systems personnel with special privileges.

The PKI Operations trusted roles include:

i. the Operations Manager;
ii. AS Operators;
iii. RA Operators;
iv. Registration Officer(s) (RO); and
v. Security Officer (SO).

For operational management of the RCA and GNet CA, with the exception of the ROs, each of the above positions requires access to the secure PKI operations facility. Privilege to access this area is controlled by the Operations Manager, based on a number of factors including the risks of human error, theft, fraud, or facilities misuse. The Lead Agency can authorise the Operations Manager the right to limit, restrict, or extend access privileges to PKI resources. These access privileges include to PKI rooms and facilities, network resources, and infrastructure components.

For the RCA and key generation ceremonies, the pivotal highly trusted roles[17] are that of the "Master of Ceremony" and "Trusted Custodian(s)" (typically no more than two). The "Master of Ceremony" should be a CISO, ITSM or equivalent with experience of managing security-related procedural activities within secure facilities. The MC will ensure the script for the proceedings is followed and record any digressions. The "Trusted Custodians" are to be highly trusted government agency staff, with PKI knowledge and/or experience. They are responsible for managing the system account credentials and security tokens that are not required on a day-to-day basis, but are critical to the security and integrity of the PKI. This includes the "Master User" accounts for both of the CAs, the "Security Officer" (SO) tokens and backup copies of the CA cryptographic key material.

The key generation and signing ceremony trusted roles includes:

i. Master of Ceremony,
ii. Trusted Custodian(s),
iii. Operations Manager (Ceremony Co-ordinator),
iv. PKI Auditor[18],
v. Password Auditor,
vi. RA/AS Operators,
vii. Site facility officer(s), and
viii. Official Witnesses.

[17] 'Highly trusted' infers a minimum security clearance of Confidential Vetting, though preferably Secret Vetting or better.

[18] The Auditor is not to have any substantial involvement in the key generation process itself.

These roles are described in more detail in the AoG *Key Generation and Signing Ceremony Plan*.

5.2.2 Number of persons required per task

Physical and logical access, and use of the following items will be conducted in accordance with the PSR and NZISM for RESTRICTED Classification, unless stated otherwise below:

i. PKI Root CA servers (to be protected and handled as CONFIDENTIAL material);
ii. PKI Root CA HSMs (to be protected and handled as CONFIDENTIAL material);
iii. PKI Root CA portable HDDs (to be protected and handled as CONFIDENTIAL material);
iv. PKI Subordinate CA Servers and firewalls;
v. Workstations with administrative or cryptographic administrative access to PKI servers; and
vi. Removable and portable storage media (data and configuration backups, system images, OS patch and AV updates);
vii. Subordinate CA HSMs.

Access to the Root CA systems will require a minimum of 3 personnel; noting at least one to be a government employee to assert oversight of the PKI Service Providers personnel routine maintenance operations on Root CA systems. The PKI is designed so that any two of four Operators, with any two of six smart card tokens, are required for sensitive PKI operations.

Backup, restore and key recovery tasks (for PKI component entities) will be subject to policy control.

RO operations are not subject to policy control.

Audit logs are to be maintained and reviewed regularly (typically weekly and no less than monthly) by the PKI Service Provider for unauthorised or inappropriate activity. Any discrepancy is to be investigated and if validated, is to be reported to the Lead Agency in accordance with the Incident Management Plan.

The Lead Agency will review audit logs as part of scheduled audit activities, such as C&A reviews, or at least annually if sooner.

Any area containing Hardware Security Modules (HSM), servers or other hardware relating to the critical PKI system components are contained in a secure area, protected at CONFIDENTIAL.

5.2.3 Identification and authentication for each role

Irrespective of the role or the tasks performed all access to PKI facilities and systems require identification, authentication and appropriate security clearance of the individual(s) involved in accordance with the Information and Communications Technology Security Policy (ICTSP) and System Security Plan (SSP). Once authenticated, the appropriate facility or system controls will determine the role, or roles, permitted for the individual(s).

The relevant CP identifies the method of identification and authentication of the end entity.

Access to secure facilities housing New Zealand Government PKI systems is to be controlled in accordance with the PSR/NZISM, and access to the PKI systems is to be further restricted to pre-authorised personnel. Photo ID and signature are required to verify the identity of all personnel accessing these PKI systems. All RO's, SO's and RCA Operators require the use of smart card tokens to perform sensitive PKI operations. See also Section 5.1.2.

5.2.4 Roles requiring separation of duties

This CPS prohibits personnel from auditing or authorising a task that they were responsible for.

All tasks accessing the RCA require multiple operators; and tasks that access the RCA private keys or HSMs require additional independent oversight by government (Lead Agency) staff.

An RO cannot authorise their own application for a certificate. A single AS Operator cannot carry out the recovery of subscriber's private keys.

An AS Operator carrying out SO duties cannot conduct an audit on work they carried out.

The duties of each role are documented in the CA Operations Manual.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All personnel in PKI positions of trust require clearances in accordance with the PSR and are to be appropriately qualified and experienced for their roles.

No formal academic or professional qualifications are required for Lead Agency or other government staff involved in the New Zealand Government PKI Framework. Although all personnel involved in the New Zealand Government PKI Framework are to be suitably experienced and competent in ICT/cyber security techniques and processes, and familiar with the NZISM. They should be able to demonstrate higher than average experience in ICT security roles, or hold suitable qualifications.

Approved PKI Service Providers are expected to demonstrate appropriate PKI knowledge and/or experience in their operational staff, including professional or appropriate academic qualifications as appropriate.

5.3.2 Background check procedures

Background checks are part of the Government security clearance process, which is required for all trusted roles. Approved PKI Service Providers may require the Lead Agency to sponsor their PKI operational staff in obtaining the appropriate security checks/clearances.

5.3.3 Training requirements

All PKI personnel will be suitably trained in relevant policy, procedure and technology, and have an understanding of PKI Standards and the New Zealand Government PKI Framework.

Government PKI nominated individuals may be employed by any agency, though are expected to have at least 2 years experience in PKI, PKT or related areas.

The Operations Manager will maintain competence in all operations areas.

Specific training for the SO will focus on security management, system auditing and system specific security applications employed in the PKI (surveillance, access systems, etc.).

AS and RA Operators are to develop and maintain an awareness of security policies. Specific training requirements are detailed in the SSP. In general, PKI personnel are to complete training in:

i. basic PKI concepts;
ii. use and operation of PKI software, hardware and associated applications;
iii. computer security awareness and procedures;
iv. privacy procedures and considerations;
v. disaster recovery and business continuity procedures;
vi. risk management procedures; and
vii. the PKI operational policies, plans and procedures.

RO training will focus on affiliation and *Evidence of Identity* (EOI) validation, registration software operation and procedures.

Training will occur:

i. when personnel commence their employment;

ii. whenever new policies and/or procedures are implemented; and
iii. whenever remedial or other training is deemed necessary by the SO and/or the Operations Manager.

PKI staff are encouraged to undertake training activities that will assist them to carry out their duties and improve the security and integrity of PKI operations. The Operations Manager may allocate and assign staff members to any suitable training activity, such as:

i. training on the use and features of new/latest release of PKI application software, and the associated database software;
ii. training on new/latest release security tools (such as firewalls, routers, application platform security, intrusion detection systems, foot print analysis tools, backup utilities etc.);
iii. training on PKI internal processes and procedures; and
iv. training on internet security, PKI, and similar topics.

Note that the training topics are to be related to the PKI business plans and activities.

5.3.4 Retraining frequency and requirements

All PKI personnel require ongoing assessments and training updates to maintain currency with policy, procedure and technology. Training on the security policy and procedures occurs annually for all trusted roles. Refer to SSP for more information.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorised actions

Unauthorised actions are identified in the Approved Documents.

The Operation Manager's response to unauthorised actions is to take into account whether the misuse was an accident, omission, or malicious act.

Where a staff member has been found to have seriously misused the resources to which they have been granted access, these actions are to be documented and passed to senior line managers, who may take administrative or disciplinary action, if appropriate. In all cases, the organisation is to inform the Lead Agency within 2 business days of the findings. See also Section 5.7.

Sanctions against contract employees, or other third party providers (e.g. Data centre facility providers), are to be in accordance with the terms and conditions of their contract, or equivalent SLA or other agreement.

Depending on the nature of the actions, sanctions will comply with New Zealand Government policy for administrative or disciplinary action and may range from counselling and/or suspension of access rights, through to dismissal and/or legal action.

In the most extreme of cases, unauthorised actions may constitute terrorist or criminal activity and result in criminal proceedings under appropriate New Zealand legislation.

5.3.7 Independent contractor requirements

For the purposes of this CPS and the New Zealand Government PKI Framework, independent contractors are subject the same provisions as permanent staff. Failure to adhere to the code of conduct and this CPS will result in the summary termination of the contract.

All contractors with physical or logical administrative access to the PKI facilities are to have either; appropriate clauses in their contract; or sign a Confidentiality/Non-Disclosure Agreement before they are allowed access to PKI systems. Casual PKI staff and third party access that are not already covered

by an existing contract (containing the Confidentiality Agreement) may be required to sign a Confidentiality Agreement before being granted limited access to information processing facilities.

No unauthorised third party will have access to the sensitive and core functions of the PKI system. This includes, but is not exclusive to:

v. changing a security parameter of one of the CA's (such as CRL publishing),
vi. key signing or generation,
vii. access to private keys (such as restoring CA key material if HSM is damaged or tampered with),
viii. recovering the key material for an RA Operator (for example, following a stolen or lost token).

5.3.8 Documentation supplied to personnel

All personnel working on the New Zealand Government PKI Framework are to be provided with a copy of this CPS and respective organisations Code of Conduct. All Lead Agency staff will adhere to the Department of Internal Affairs Code of Conduct.

For each role, the personnel performing duties, procedures and responsibilities receive access to the necessary documentation for that role. All documentation will be available within the PKI facilities for access by operational staff.

ROs will only be supplied with relevant documentation for the registration of Subscribers, though they are also to be familiar with this CPS, as well as the Incident Management Procedures and DRBCP.

Access to data and reports is subject to Government security classification controls [PSR].

5.4 Audit logging procedures

5.4.1 Types of events recorded

Records of RA and CA infrastructure events are to include:

i. all successful and rejected network connection requests;
ii. all successful and unsuccessful logins;
iii. all certificate requests received;
iv. administering and configuring the PKI system components;
v. administering and configuring privileged user accounts (including permission changes); and
vi. significant certificate lifecycle events.

Significant certificate lifecycle events include, but not necessarily limited to:

i. RCA and Subordinate CA Key generation,
ii. RCA private key use,
iii. signing-key generation requests (new CA accounts),
iv. certificate generation requests,
v. certificate propagation to PKI Service Providers and other bilateral interoperability partners,
vi. key destruction requests,
vii. key destruction verification reports,
viii. CRL notifications,
ix. bilateral (interoperability) certificate revocation notifications,
x. private key removal,
xi. tamper detection with private key devices (e.g. HSMs),
xii. certificate signer and RO console access, and
xiii. certificate signer and RO private key use.

The recorded log information shall include a minimum of:

i. date/time stamp;

ii. event target;
iii. event source;
iv. event description; and
v. CA/RA event status (Success/Failure).

5.4.2 Frequency of processing log

Audit logs require processing **at least monthly** for anomalous and unauthorised events. Processing is to include searches for anomalous patterns across more than one month. Additional processing will be performed as required if an incident occurs warranting an investigation of events leading up to incident.

RO / RAO logs certificate generation console logs are to be reviewed **Weekly** for evidence of tampering or unauthorised access.

RCA and CA key generation/signing event logs are to be reviewed at the start and end of every certificate generation ceremony.

RCA system and access logs are to be reviewed at the start of every event that requires them to be run-up.

Audit logs will be audited at least annually[19].

5.4.3 Retention period for audit log

Audit retention/ backup and archival policies are to ensure that together a complete record of all audit material is maintained, and recoverable for a minimum period of 7 years, as specified in the New Zealand Public Records Act 2005 (PRA), or for the remaining life of the respective CA Certificate, whichever is longer.

Additional requirements are to be detailed in relevant CP and Subscriber Agreement (i.e. where a subscribing agency has regulatory or legal requirements that exceed or override the above).

All New Zealand Government PKI Root CA (RCA) audit logs are to be retained and recoverable for a period of 7 years after the expiration of the Root CA Certificate life[20].

Backups of audit logs are retained for 12 months.

Disposal of audit logs is to be in accordance with the PSR, or the relevant government policy on destruction of media at the time.

5.4.4 Protection of audit log

Protection of Audit log information is in accordance with the PSR for the protection of security log information for systems processing RESTRICTED information.

Audit logs may only be viewed by RA Operators (RAO), the Operations Manager, Trusted Custodians or the PKI Auditor. The logs are protected from modification and are not to be deleted.

Audit logs are to be protected from modification and deletion, using such mechanisms as Access Control Lists (ACL) techniques and off-system secure storage (e.g. HSM).

5.4.5 Audit log backup procedures

Backups of Subordinate CA and RA audit logs occur daily.

Backups of Root CA audit logs are to be conducted as part of all Key Generation and Signing Ceremony procedures; and CRL renewal activities (i.e. at least 6 monthly).

[19] Providers conduct internal audits at least annually. Lead Agency will seek to independently audit at least every 2 years.

[20] Initial Root CA Certificate expiry is April 2026; hence audit logs would need to be retained till at least April 2033.

Where log information processing into a common format for analysis occurs, both raw and processed log data are required to be backed up.

5.4.6 Audit collection system (internal vs. external)

The audit collection system is a combination of automated and manual processes performed by the operating system and operational personnel.

Audit logs are to be exportable from the host system and able to be manually reviewed (human readable), but not altered.

5.4.7 Notification to event-causing subject

Operations personnel shall notify the Operations Manager or SO in the event of a process or action causing a critical security event or discrepancy.

Any event signalling tampering with the certificate signing device, any of its private keys or associated core components are to be treated with highest priority. Such events are to be notified to the SO for action within 15 minutes of the alert being detected. Once confirmed, the Lead Agency must also be notified immediately.

Approved Service Providers are to ensure all CA and RA critical incidents concerning potential compromise or breach are reported to the NCSC, and all related logs to be made available to the NCSC for analysis.

The Lead Agency is to notify the NZ CERT of confirmed compromise incidents, where appropriate.

5.4.8 Vulnerability assessments

Vulnerability assessments are to be conducted in accordance with New Zealand Government policy and industry best practice. Vulnerability assessments are to include network level infiltrations; physical infiltrations; and personnel operations assessment, for both the PKI Service Provider and dependent third party suppliers (e.g. data centre facility management). Appropriately qualified individuals from the AoG Security and Related Services (SRS) Panel[21] are to be used to conduct security vulnerability assessments[22].

5.5 Records archival

5.5.1 Types of records archived

All audit log records for RCA, Subordinate CA and RA infrastructure and key generation activities require archival (see Section 5.4.1 for typical event types) in accordance with New Zealand Archive Standard and Public Records Act 2005 (PRA).

All RCA and CA key generation master ceremony scripts and signatory sheets are to be archived by the Lead Agency.

All RCA CRL instances are to be archived and retained for the life of the RCA, or in accordance with PRA timeline requirements (currently 7 years), whichever is longer.

To minimise the duplication of records, duplicated archives are destroyed, whilst maintaining a full record of all auditable events. See Section 5.4.3 for management procedures.

Archiving of key material is required for specific components to support the archiving requirements for the PKI. That is, in order to access information from archived PKI databases, a set of specific key material is required to be archived and stored securely along with the archived PKI databases.

[21] https://www.digital.govt.nz/products-and-services/products-and-services-a-z/ict-security-and-related-services-panel/

[22] Though PKI WebTrust assessors and testers are not specifically covered by the SRS Panel arrangements and are likely to have to be sourced from overseas.

The specific components of key material generated for archive includes:

i. archive RCAOs when RCA database is archived;
ii. archive Sub-CAOs when Sub-CA database is archived; and
iii. archive *CMS Auditor* when CMS database is archived.

5.5.2 Retention period for archive

The periods stated at Section 5.4.3. also apply to archive records.

5.5.3 Protection of archive

Archive media is protected by physical security and cryptographic protection commensurate with the security classification of the contents and in accordance with the provisions of the PSR.

5.5.4 Archive backup procedures

Archive data backup is in accordance with the respective Approved PKI Service Providers PKI Backup procedures and technical guides. The archive backup procedures should also be aligned with respective providers DRBCP.

5.5.5 Requirements for time-stamping of records

Individual events shall be time stamped with the timing of the event. Audit logs shall also be time stamped with the time of archival, and if via a backup process a timestamp of the relevant backup.

5.5.6 Archive collection system (internal or external)

Archiving is performed by AS Operations personnel.

Key pairs will be archived and retrieved using the procedures documented in the KMP.

5.5.7 Procedures to obtain and verify archive information

To provide authentication and integrity confirmation of the archive records, digital signatures are applied.

5.6 Key changeover

A change to the New Zealand Government PKI Framework Root CA's (RCA's) keys will require re-key of all subordinate certificates in the certification path. The Lead Agency will, within reason, inform all Approved PKI Service Providers and Subscriber Agencies (through respective Subscriber Authority) of any RCA or Subordinate CA key changeover in advance and may revoke, reissue or re-key subordinate certificates as circumstances require it.

The Lead Agency is under no obligation to inform individual Subscribers of any RCA or Subordinate CA key changeover in advance. This responsibility rests with respective Subscriber Authorities and Approved PKI Service Providers.

The New Zealand Government PKI Framework ensures that the key changeover process and procedures will provide for uninterrupted operation of the RCA and Subordinate CAs managed under this CPS, and will also ensure that subordinate certificates do not become invalid as a result of CA key changeover.

Key changeover periods will be in accordance with policy, and prior to normal certificate/key expiry.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

All security incidents (as per the DRBCP) are to be logged, and an investigation of the incident is to be undertaken, to determine if:

i. key or CA systems compromise has occurred, is suspected, or cannot be discounted;
ii. the incident was deliberate or accidental;
iii. procedures require to be modified, to address the circumstances that enabled the incident to occur; and
iv. any further action is required.

If it is possible that a key compromise has occurred, the certificate requires revocation. All cross-certified CAs are to be informed if an applicable CA is compromised.

The decision to revoke the certificates subordinate to the compromised entity is optional however; the AS Operations Manual describes the necessary processes. Where a *superior CA* is compromised, ALL immediately *subordinate CAs* are effectively revoked.

The Lead Agency will receive notification of all incidents where the continued integrity of service is impacted, and will provide a formal notice to cross-certified entities, and accrediting bodies, indicating the proposed corrective action and the estimated schedule for implementation.

The NCSC and NZ CERT are to be notified of critical compromise or system breach incidents, in accordance with Sect 4.9.12 and 5.4.7, for subsequent forensic investigations

The PKI providers will undertake a "cold" disaster recovery exercise at least once a year, including restore from backups. The PKI components are to be able to be recovered to a state no more than one week out of date in the event of a regional disaster. The Lead Agency is to be informed, and ideally involved as observers, of such exercises.

The Approved Service Providers PKI DRBCP is to detail the restoration strategy for most common serious incidents or disasters.

5.7.2 Computing resources, software, and/or data are corrupted

The backup of *private signing keys* for CAs occurs only if appropriate protection applies, and is only used as part of a rebuild if compromise has not occurred or is not suspected.

5.7.3 Entity private key compromise procedures

If the entity private key is compromised it is revoked and the entity is to re-apply for registration.

A Subscriber who becomes aware of key compromise is to immediately notify their Subscriber Authority and be prepared to assist in revoking affected certificates without delay.

5.7.4 Business continuity capabilities after a disaster

Follow the procedures in the respective PKI DRBCP.

Priorities for Business Continuity are in the following order:

i. personal safety of all staff;
ii. physical investigation of disaster and collection of necessary evidence to complete investigation – sign off as required by Lead Agency;
iii. re-establishment of secure environment for PKI operations – temporary measures are acceptable but require detailing in the PKI DRBCP or sign off by the Lead Agency.
iv. reconstitute the ability to issue CRLs and process revocation requests – this includes audit functionality;
v. reconstitute the ability to receive, process and issue certificates;

vi. return to stable operating conditions;
vii. update documentation to reflect any changes as a result of recovery – including to processes, procedures and configuration; and
viii. provide an incident closure report to the Lead Agency.

5.8 CA or RA termination

In the event of a CA or RA termination, or a CA or RA ceasing operation, its certificate requires revocation. Self-signed CAs (including the RCA) shall follow notification procedures equivalent to key compromise. Termination of CAs, where possible, are to minimise impact on subordinate certificates.

The Lead Agency receives notification of planned and actual terminations.

Only the Lead Agency can authorise the termination of the RCA.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation for the RCA is to be via a combination of product and process approved by GCSB and the Lead Agency.

Key pair generation is to be via a combination of product and process approved by the Lead Agency to provide keys suitable:

i. for use in PKI based authentication, non-repudiation and integrity services for systems; and
ii. for use in PKI based confidential communications capable of protecting symmetric (Private Key encryption) keys used to protect data up to and including RESTRICTED over publicly accessible or other untrusted data networks (e.g. the Internet).

See relevant CP for description of key pair generation.

The PKI CKMP details the products, process and procedures and the approved combinations, which are valid.

The RCA's signing key is generated and secured by an *offline* Hardware Security Module (HSM).

Subordinate CA keys are also to be generated and secured by a HSM (typically *online*).

The RA signing key is to be generated on suitably secured tokens, and the encryption key generated by the CA software. The RA keys can both be stored on the token, though the enhanced physical access and procedural controls apply as per this CPS.

6.1.2 Private key delivery to Subscriber

Private key delivery is defined in the relevant CP.

6.1.3 Public key delivery to certificate issuer

Public key delivery is defined in the relevant CP.

6.1.4 CA public key delivery to relying parties

Public keys for a CA in a certificate chain for entity certificates will be accessible to Relying Parties using the approved repositories.

In addition, CA certificates in the chain which are self-signed (e.g. RCA) will be delivered, using secure methods approved by the Lead Agency to third party CAs, where a cross certification (or equivalent) agreement is in place.

Subscribing Agencies will have relevant certificate chains installed into the Certificate store on workstations and servers within their enterprise architecture infrastructure.

6.1.5 Key sizes

Key sizes are defined in the CKMP and relevant CP.

The New Zealand Government PKI Framework overarching encryption algorithm key sizes meet the requirements of the NZISM and are detailed in the *New Zealand Government PKI Framework* document.

6.1.6 Public key parameters generation and quality checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Public key parameters shall be generated in accordance with NZISM, as defined by the Lead Agency.

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with the NZISM, or other GCSB approved guidance.

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

Subscriber certificates include key usage extension fields to specify the purposes for which the keys may be used and also to technically limit the functionality of the certificate when used with X.509v3 compliant software. The correct values for key usage are set in these fields in accordance with the X.509v3 standard, though the New Zealand Government PKI cannot control how third-party software applications interpret or act upon these. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of the New Zealand Government PKI.

Keys may only be used in compliance with this CPS, and all restrictions described in this CPS are to be observed. The Key Usage field provides an indication of acceptable usage, regardless of whether this field is technically utilised by an application. Designating this extension as non-critical does not indicate any reduced need for compliance.

See the relevant CP for key usages.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

All cryptographic modules used with PKI core components comply with NZISM requirements, specifically in complying the Common Criteria scheme Evaluation Assurance Level 4 (EAL4) and US Federal Information Processing Standard Publication 140-3 (FIPS-140-3) requirements. Cryptographic modules are to be listed on the New Zealand Government Evaluated Products List or approved for the uses intended in this CP by the Lead Agency and GCSB.

The PKI RCA core components (hardware and software) are to be protected and handled as CONFIDENTIAL classification regulations, and are to be evaluated and approved by GCSB against the appropriate target operating environment for the New Zealand Government PKI Root CA prior to initial use.

Sub-CA and RA cryptographic modules for the uses intended in the respective CP are to be compliant with the NZISM requirements and are to be checked as part of the Certification audit process.

The Approved Service Providers PKI Build and Configuration documentation are to detail the products used.

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

All CA and RA operations involving generation of Private Keys require a minimum of 2 persons and a minimum of two *m-of-n* access factors to private keys (on HSMs)[23], each with unique passcodes.

A minimum of two passwords, passphrases or passcodes are required to access all critical PKI components handling private keys (e.g. HSM, CA servers, etc.); and are to comply with, or exceed, NZISM password structure and management requirements.

All CA and RA operations involving generation of Private Keys by the Root CA (RCA) and GNet Shared Policy CA (operated by Cogito Group), require a minimum of 2 persons, and access to private keys (on HSMs) requires 2-of-6 smart card token authorisation, each with unique passcodes.

The Authentication Services Operations Manual and SSP are to ensure that CA and RA key certification requests require two authorised operators to generate. Key generation of PKI entities (CA and RA components) are to be conducted in a suitable secure area, requiring multiple personnel from Lead Agency, subscribing agencies and the Service Provider, to fulfil specific roles for key ceremony. The mandatory roles are listed in the New Zealand Government PKI CA Key Generation Ceremony procedure.

RCAs are to be offline[24] at all times. Access to the RCA for CA key generation requests and self-certification requests require a minimum of 3 personnel, with at least one being a government employee[25]. All are to hold minimum of CV or higher security clearance, with at least one person in a management role holding SV or higher clearance.

Subordinate CA systems are to have a minimum of 2 personnel trained and authorised in PKI, with security clearances at least one state above that of the subject CA or consuming system (i.e. CV for a RESTRICTED Sub-CA)

No single person is to be able to fully access and operate any components of the PKI systems that contain or generate Private Keys, RCA or CA Certificates, and RCA CRL generation.

6.2.3 Private key escrow

Private Keys are stored on respective CA server hardware with access and encryption protection controls secured by HSMs.

Escrow of end entity private authentication keys does not occur.

The relevant CP details whether private confidentiality keys are subject to escrow.

6.2.4 Private key backup

Back up of end entity private authentication keys does not occur. Where such keys must be transferred to other media for disaster recovery purposes, they are transferred and stored in an encrypted form protected by the HSM keys.

Critical PKI components, such as CAs and RAs, have duplicate private keys created. Where these keys are stored on hard tokens, the archive copy is also to be a hard token.

All components of the backed-up key are to be stored in a separate, geographically dispersed site.

[23] Eg. use of 2-of-6 smart card tokens for operator authorisation for the RCA and GNet Shared Policy CA.

[24] 'Offline' refers to not being connected, or being functionally able to be connected, to a network. This requires Ethernet and wireless network adapters to be disabled or removed from Root CA components.

[25] Lead Agency to provide, though participants can be drawn from across subscribing agencies and the AoG PKI Technical Advisory Group (TAG) membership.

Duplicated hardware security tokens are recorded within tamper evident envelopes and signed by the SO.

Key components and access codes are to be stored and transported separately in individual sealed envelopes, within approved security containers or safe-hand bags.

Backup key components will be retrieved from storage upon expiry of their key usage period, securely erased and destroyed under supervision by the PKI Auditor and/or Lead Agency representatives.

6.2.5 Private key archival

Archive of end entity private authentication keys does not occur.

Private keys will not be archived upon expiry of their key usage period, and devices containing backup key components will be destroyed.

6.2.6 Private key transfer into or from a cryptographic module

The transfer of private authentication keys from, or into, a cryptographic module does not occur except for the duplication of keys for the PKI core components. Where this occurs it is done by a product on the GCSB/ASD Evaluated Product List[26].

Any confidentiality keys that are transported into or from the cryptographic module are transferred using the PKI Software confidentiality key(s).

RA Operator and subscriber keys cannot be exported from hardware tokens.

6.2.7 Private key storage on cryptographic module

All private keys will be generated and stored by dedicated and GCSB approved cryptographic modules, relevant to the Classification of the CA and Certificates associated with the private keys.

Within the PKI environment in general, private keys are either stored encrypted, stored protected by a password, or stored password protected in hardware (such as an HSM, USB token, or smart card).

The private keys are stored in a protected secure facility and only accessible with the cryptographic module (i.e. HSM).

Private keys generated by, and directly associated with, the Root CA are to be stored, accessed and managed as CONFIDENTIAL material.

6.2.8 Method of activating private key

See relevant CP.

6.2.9 Method of deactivating private key

Deactivation of private keys is in accordance with a method approved by GCSB (for the RCA components) or the Lead Agency (for all Subordinate CAs) and summarised in the relevant CP.

Private keys are deactivated by expiry of their key-usage period.

Private keys used in HSMs are deactivated when the HSM is powered down. Operator hard tokens are removed from the token reader (deactivating access) and stored in accordance with the PKI ICTSP, PKI SSP and PKI KMP. The DRBCP details recovery methods and timelines for private keys in the event of a disaster or other incident (e.g. PKI facility power failure).

6.2.10 Method of destroying private key

PKI positions of trust can destroy private keys.

[26] Where an HSM is used to transfer keys, the 'Data Export Key' must be stored in such a way that multiple (e.g. 3 of 6) tokens used to store it must be used together to recreate this key inside the HSM, and consequently import and decrypt the original HSM key material contents.

Cryptographic HSMs, hard tokens and key storage locations will be re-initialised (or 'tampered' with) to destroy the stored private keys. Other transportable media or non-cryptographic devices are to be physically destroyed (i.e. made 'beyond use').

Subscribers may destroy their own authentication private keys when no longer needed either by securely erasing/destroying the token, or by having their hard token re-initialised.

6.2.11 Cryptographic module rating

See 6.2.1 (Cryptographic module standards and controls) of this CPS.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Archive of end entity public authentication keys does not occur.

6.3.2 Certificate operational periods and key pair usage periods

Within the PKI certificate lifetimes are nested and as such the key lifetime is dependent on the certificate life. In other words, an issued certificate (of an end entity or a CA) expires before the certificate of the CA that issued it. Otherwise, after the CAs expiration, the issued certificate becomes invalid, even if it has not expired.

Key lifetimes are set as a matter of policy and will typically depend on a number of factors, including the algorithm type and size of the key. As such the key lifetimes are detailed in the PKI KMP and the applicable CP specifications.

6.4 Activation data

6.4.1 Activation data generation and installation

See relevant CP.

6.4.2 Activation data protection

All passphrases used to activate the private key shall be kept in accordance with the CKMP

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The core components of the PKI system, including RCA, HSMs, and other modules that handle private keys, are to meet New Zealand security standards, including:

i. Common Criteria EAL4 (or higher),
ii. FIPS PUB 140-2 for non-cryptographic hardware,
iii. FIPS PUB 140-3 for cryptographic modules (e.g. HSM), and
iv. GCSB/ASD Evaluated Products List.

Cogito Group has established an ICT Security Policy (ICTSP) and System Security Plan (SSP) for the computer security technical requirements for:

i. New Zealand Government Root CA (RCA);
ii. AoG Shared Policy CA; and
iii. Authentication Service operations, for TaaS GNet.

These are controlled documents for internal use only and are only available to appropriately cleared personnel on a controlled basis.

The Government RCA security requirements documentation may be provided to Agencies and other Government PKI Service Providers upon approval by the Lead Agency[27].

Appropriate levels and balance of trustworthiness and security exist throughout the New Zealand Government PKI. Security meets New Zealand Government requirements for systems cleared to store and process data that is RESTRICTED and Below, which meets or exceeds the requirements mandated for a PKI *High Assurance* service.

The RCA systems are a unique case within the PKI, being handled, managed, stored and operated as CONFIDENTIAL systems. Though the highest classification level of any single information component (including private keys) in the RCA systems is to be no higher than RESTRICTED.

Controls in place include:

i. PKI system security ownership and roles allocated;
ii. a configuration baseline and a configuration change control process;
iii. performance of regular and frequent systems operability tests to prove the correct operation of critical PKI components;
iv. strong authentication and access control required for core PKI system access (including remote access);
v. proactive user account management including comprehensive auditing and timely removal of access;
vi. role segregation and application of strict policy procedures;
vii. organisational segregation and policy controls for the RCA systems (i.e. Service Provider personnel cannot access the systems without government personnel being in attendance);
viii. multiple organisations and personnel required to conduct Key Generation and Signing Ceremonies, with robust procedure controls;
ix. restrictions and controls on the use of system utilities;
x. hardening and accredited OS and firmware used as per NZISM and GCSB guidance;
xi. patch management, including OS, AV and malware protection (as per ASD Top 4 mitigations and NIST CSC)[28];
xii. the use of monitoring and alarm systems to detect and warn of unauthorised access to computer system resources;
xiii. logging of all system access and use; and
xiv. regular internal reviews and independent audits by Approved PKI Service Providers and Lead Agency.

6.5.2 Computer security rating

All facilities and equipment have been constructed or selected to satisfy appropriate PSR and NZISM security requirements, as per Section 6.5.1.

6.6 Lifecycle technical controls

6.6.1 System development controls

The software development controls applied in the development of the CA software has been evaluated and certified to meet, or exceed the requirements of ITSEC E3 or Common Criteria EAL4.

[27] Usually the SSP (and ICTSP optional) are contained in the C&A Certification pack.

[28] This also includes all offline components of the PKI environment, such as the Root CA servers. Though offline components only require patch updates applying when accessed (powered up and operated), not as a matter of business as usual update schedules.

Changes in the production environment are tested in the PKI test environment, which is operated and maintained within a physically secure environment. Proposed changes are then approved for deployment by the Lead Agency in accordance with the PKI Change Control Management Procedures.

6.6.2 Security management controls

Security management controls exist to ensure that PKI systems are operating correctly and in a manner consistent with the PKI configuration baseline. The configuration baseline document includes a schedule of configured items, including details of the hardware and software configuration parameters and a mechanism for identifying appropriate documentation and known security flaws for each item.

The Operations Manager is responsible for maintaining the configuration baseline and for managing any changes in accordance with the SSP. The SO is responsible for maintaining a change control process at the PKI that records all changes to the PKI configuration, including all hardware and software changes.

Security management controls are described in further detail in the SSP.

Lead Agency regular audits are to check the baseline configuration matches the actual system components deployed and the change control register.

6.6.3 Lifecycle security controls

All the PKI RCA components are to be considered and managed as CONFIDENTIAL security classification, to maintain the integrity, assurance and trust of the PKI Framework.

All Subordinate CA's and associated RA's are to be considered and managed as RESTRICTED security classification.

Regular internal reviews and independent audits are to be conducted by Service Providers and Lead Agency.

6.7 Network security controls

The RCAs are maintained as offline systems and are not to be connected to networked environments under any circumstances; hence network security controls are not applicable. All data transfer for RCAs is to be via removable, write-once, media (e.g. CD-R, DVD-R).

The New Zealand Government PKI network security controls for online Sub-CA's include:

i. firewalls;
ii. strong authentication and technical access controls;
iii. enhanced physical and third-party personnel access controls;
iv. resilient, secure and appropriately containerised network architecture and configuration;
v. strong management traffic protection;
vi. mechanisms to prevent denial-of-service attacks; and
vii. password and other logical access control.

The network security controls for the PKI environments were developed in accordance with the NZISM, after conducting an appropriate threat and risk assessment. The risk assessment and Certification report for the RCA is available to New Zealand Government PKI Service Providers[29] and Subscribing Agencies to review as part of their own risk assessment and service Accreditation requirements. See Section 8 for details of the C&A processes.

[29] Currently through the TaaS Managed Security PKI Services Tower approved suppliers.

PKI network services are operated and maintained within the physically secure environment of the PKI. AoG Infrastructure as a Service (IaaS) facilities are to be used in preference to other facilities, in order to simplify the C&A and audit requirements.

The PKI Subordinate CA network is a discrete network, controlled from the PKI Facility. The only network traffic allowed is from authorised PKI entities and essential core services such as directories, time and synchronisation with any back-up or alternate sites. All other traffic is denied by default. PKI management traffic is to be protected in transit in accordance with NZISM requirements.

6.8 Time stamping

No trusted time sources or other external time-stamping services are used for the RCA or associated Subordinate CAs.

There are presently no identified requirements for trusted time stamping of certificates, or signature requests, in the New Zealand Government PKI Framework.

Audit log entries record current system time with every entry, and RCA system clocks are set according to a reasonably accurate wall clock provided in the key generation ceremony secure facility.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Appendix D contains a list of OIDs[30] (for CPs) approved to operate under this CPS. The relevant CPs detail the specific Certificate, CRL and OCSP profiles.

Accreditation processes ensure that this CPS is suitable for a CP, prior to the CP being approved for use by the Lead Agency.

Cogito Group will maintain the CRL for the New Zealand Government PKI on behalf of the Lead Agency.

CRL updates will be issued at least every 180 days (6 months), but not more frequently than every 5 days.

Revocation of the RCA certificates is to be through out-of-band processes and systems, and not through the New Zealand Government PKI.

7.1 Certificate profile

7.1.1 Version number(s)

CAs operating under this CPS shall only issue X.509 Version 3 certificates.

7.1.2 Certificate extensions

See relevant CP.

7.1.3 Algorithm object identifiers

See relevant CP.

7.1.4 Name forms

Distinguished Names (DN) will be used by the CAs in the issuer and in subject fields of the certificates. The DN shall not be blank. Directories use the DN for lookups. Names are to be meaningfully related to the identity presented for EOI check and relate directly to the identity of the subscriber, except as otherwise provided in the relevant CP. Some communities or installations may choose to use other names, for example, certificates used to implement a hardware protocol, where device addresses are

[30] Appendix C outlines the New Zealand Government PKI Framework object identifier (OID) structure.

more useful. In this case, an alternate name form may be included in the subjectAltName extension. Use of alternate name forms shall be in accordance with the CP, including criticality, types, and name constraints. The combination of DN and subjectAltName must be unique within the PKI.

See relevant CP for name forms.

7.1.5 Name constraints

See relevant CP.

7.1.6 Certificate policy object identifier

See Appendix C for the New Zealand Government PKI Framework OID structure.

Refer to relevant CP for details.

7.1.7 Usage of policy constraints extension

See relevant CP.

7.1.8 Policy qualifiers syntax and semantics

The certificate policies extension will be used to clearly indicate the policy under which the RCA and CA certificates have been issued and the purposes for which the certificates may be used.

See relevant CP.

7.1.9 Processing semantics for the critical certificate policies extension

See relevant CP.

7.2 CRL profile

7.2.1 Version number(s)

CRLs for certificates issued under this CPS shall assert a version number as described in the X.509 standard [ISO/IEC 9594-8:2014]. CRLs shall assert Version 2.

7.2.2 CRL and CRL entry extensions

See relevant CP.

7.3 OCSP profile

7.3.1 Version number(s)

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

7.3.2 OCSP extensions

All OCSP extensions are to comply with RFC 6960.

OCSP certificates are issued with the no-check extension (id-pkix-ocsp-nocheck), negating the need of the relying party to validate the OCSP responder's certificate through another source such as the CRL. This extension will not be marked critical.

Refer to the X.509 Certificate Policy for New Zealand Government Validation Authority Certificates [VA CP] for a full OCSP profile.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The New Zealand Government PKI is subject to the Government Certification and Accreditation (C&A) procedures, based on the AoG Common Capabilities and Telecommunications as a Service (TaaS) C&A Framework [NZISM compliant].

The RCAs will be subject to a separately documented process than the Subordinate CAs and RAs:

i. **RCAs and the 'Shared Policy CA'** are 'Certified' and 'Accredited' by the Lead Agency in conjunction with GCSB endorsement and oversight, in recognition of the CONFIDENTIAL nature of the RCA systems. RCAs are protected, managed and handled as CONFIDENTIAL, though Subordinate CAs provide pan-government information protection at RESTRICTED and Below.

ii. For **Subordinate CAs and RAs**, the AoG TaaS C&A Procedure will apply. 'Certification' activities, including conduct of a threat and risk assessment, and review of artefacts listed in the Approved Documents table, are to be conducted by respective PKI Service Providers. The Lead Agency will 'Accredit' these PKI services, noting each subscribing agency retains the right to conduct independent Accreditation activities where appropriate.

All infrastructure elements in the New Zealand Government PKI, including the RCA, CAs and RAs, require auditing on a regular basis to ensure that they comply with this CPS, relevant CPs and the NZISM. The process of such audits is not publicly disclosed.

In addition to the CPS requirements, accreditation requires Service Providers to conduct independent annual PKI audits to ensure compliance with Lead Agency policies and criteria. Such audits are to be performed by an approved member of the AoG Security and Related Services (SRS) Panel, and they should use a recognised framework; such as the AICPA/CICA WebTrust Program for Certification Authorities [see References]; to set criteria to be used as a basis for an auditor to conduct a PKI baseline audit.

The Lead Agency gives further consideration to the results of all audits before implementing any recommendations[31].

8.1 Frequency or circumstances of assessment

Service Providers are to ensure each CA and RA are subject to an annual audit, more frequently if required under the following circumstances, by an approved auditor (see Section 8.2) to assure that they comply with this CPS and relevant CPs.

The Lead Agency is to conduct PKI audits for the following events:

i. On handover / takeover of administrative responsibility, or ownership for the system,
ii. On change of individuals with access to the PKI systems cryptographic components,
iii. On establishment of new PKI Subordinate CA to the framework by approved Service Providers, or
iv. For each 12 month period the PKI Framework is in operation[32].

The Lead Agency are to ensure a full audit of all PKI service components (physical, technical, personnel, procedures) is conducted every 2 years (though no longer than 3 years), or in exception of a major change or event necessitating an earlier review, in order to maintain the formal Certification & Accreditation status of the Government PKI environment.

[31] Note: The Accredited CA is subject to direction by the Accreditation Authority in relation to maintaining accreditation.

[32] This is likely to consist of a review of the Service Providers validated independent audit reports.

An external audit may also be instigated in the event of discovery of a serious or endemic compromise, or at any time if the audit processes described above or in section 5.4 are deemed inadequate.

8.2 Identity/qualifications of assessor

General security audits will be conducted by approved vendors on the AoG ICT Security and Related Services Panel (SRS Panel)[33]. Regardless of which external auditor is commissioned, they are to have specific expertise in IT security auditing and should have demonstrable expertise in PKI auditing.

Specialist PKI Auditors are to be approved by the Lead Agency based on recognised industry certification (e.g. WebTrust certified auditor), or alternatively suitable expertise in relation to PKI, electronic signature technology, IT security procedures or any other relevant areas of expertise required of an evaluator to perform an evaluation properly and expertly against the Accreditation Criteria[34].

8.3 Assessor's relationship to assessed entity

Auditors are to be independent of the audited entity and have no actual, or potential, conflict of interest during the period of the audit.

8.4 Topics covered by assessment

The purpose of audits is to ensure that each CA and RA:

i. maintains compliance with Accreditation criteria and policies, set out in the NZISM[35];
ii. maintains compliance with the cryptographic protection and algorithm requirements for New Zealand Government PKI systems, set out in the NZISM; and
iii. continues to operate in accordance with the government policy, PKI Framework Approved Documents, and international best practices (such as the WebTrust program).

Topics covered by the assessment are based on the PKI Framework, which identifies a series of compliance audit activities that are to be performed to ensure the operational integrity and suitability of the infrastructure.

8.5 Actions taken as a result of deficiency

Auditor identified deficiencies will be presented to the Lead Agency. The Lead Agency will determine actions to be taken in relation to any deficiency. Where this deficiency affects accredited systems authorised representatives of Accreditation Agencies will be included in the review and determination of the solution.

Any deficiency that impacts upon continued accreditation is to be remedied to the standard required by the Accreditation Agency(s).

Failure to adequately address deficiencies identified in an audit in an agreed timeframe may result in withdrawal of the entity's accreditation and/or termination of the Accreditation Authority Memorandum of Agreement.

The PKI Operations Manager, or other appointed security management role, is responsible for the on-going management of the PKI accreditation.

[33] https://www.digital.govt.nz/products-and-services/products-and-services-a-z/ict-security-and-related-services-panel/

[34] WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria, V1.1, dated 2013.

[35] Noting that NZISM updates are released several times a year and compliance with the current NZISM v2.4, dated Nov 2015, is expected to be maintained with future NZISM versions no older than 2 years, or 4 revisions, whichever is the shorter period.

8.6 Communication of results

The results of an audit are confidential and require the auditor to communicate them only to authorised representatives of Accrediting bodies and the audited entity.

All required corrective action must be verified to have been completed within the agreed timeframe.

The Approved PKI Service Providers Operations Manager has the responsibility for correspondence of results of PKI audits between the PKI and other entities, for example GCSB or the Lead Agency.

Audit Certificates and associated reports and remediation plans will be provided to Subscribing Agencies (or their designated Subscriber Authority) to satisfy the subscribing agency architecture, risk assessment and C&A needs.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

See relevant CP.

9.1.2 Certificate access fees

See relevant CP.

9.1.3 Revocation or status information access fees

See relevant CP.

9.1.4 Fees for other services

No fee is levied for access to this CPS, or relevant CP via the approved repositories. Printed copies may be made available for a fee.

See relevant CP for any other service fees.

9.1.5 Refund policy

Where a fee is charged for a certificate, once that certificate is issued a refund will not be provided. The relevant CA will issue a new certificate free of charge if, through the fault of the CA, an erroneous certificate was issued.

9.2 Financial responsibility

Approved AoG (TaaS) PKI Service Providers are to have sufficient resources to meet their perceived obligations under this CPS. The associated TaaS PKI services are to be made available on an 'as available' basis.

Nothing in this CPS, or relevant CP, or the issuing of Key Pairs and Certificates under it, establishes a fiduciary relationship between the New Zealand Government PKI and an end entity, or Relying Party.

The New Zealand Government PKI is not liable for any loss or damage arising from any delay or failure to perform its obligations described in this CPS.

Relying Parties assume responsibility for any financial losses due to transactions authenticated using certificates issued under this CPS.

9.2.1 Insurance coverage

See relevant CP.

9.2.2 Other assets

See relevant CP.

9.2.3 Insurance or warranty coverage for end-entities

See relevant CP.

9.3 Confidentiality of business [controlled] information

New Zealand Government official information requires classification, handling markings, storing and processing in accordance with New Zealand Government Security policies[36]. Public access is only to information classified for release to the public domain (UNCLASSIFIED). Release of all other information will be subject to satisfying security clearance requirements and a demonstrated "need-to-share".

9.3.1 Scope of PKI controlled information

The New Zealand Government PKI provisioned under the TaaS Agreement is not to be used for the protection of government information classified at CONFIDENTIAL or above.

9.3.2 Information not within the scope of controlled information

No stipulation.

9.3.3 Responsibility to protect controlled information

Whilst the keys provided are suitable for use in PKI confidential communications capable of protecting symmetric (PKI Key encryption) keys used to protect data up to and including the RESTRICTED classification over publicly accessible data networks (e.g. the Internet), the sending party in any communication is responsible for complying with New Zealand Government Security policies.

9.3.3.1 COMMERCIAL-IN-CONFIDENCE Protective-Marked Information

Where in connection with the use of the New Zealand Government PKI, COMMERCIAL-IN-CONFIDENCE Information is provided or produced, the relevant party shall ensure that any person receiving or producing the information protects the 'commercial confidentiality' of the information, except:

i. where disclosure of the information is required by law or statutory or portfolio duties;
ii. where disclosure of the information is made to the responsible Minister or in response to a request by a House or Committee of the Parliament of New Zealand; or
iii. to the extent that the respective Approved PKI Service Provider would be prevented from exercising its Intellectual Property rights under the TaaS commercial and subscriber agreements, or other contract.

The Subscriber shall not, in marking information supplied to the Approved AoG PKI Service Providers, misuse the term COMMERCIAL-IN-CONFIDENCE or the end entities equivalent. The marking of information as COMMERCIAL-IN-CONFIDENCE shall not affect the legal nature and character of the information.

9.4 Privacy of personal information

9.4.1 Privacy plan

The New Zealand Government PKI Privacy Statement conforms to the requirements of the *Privacy Act 1993* (Privacy Act). The Privacy statement is available internally from New Zealand Government repositories and externally at http://www.pki.govt.nz.

[36] PSR is the primary policy in this area, supported by the NZISM for practical control measures.

9.4.2 Information treated as private

See relevant CP.

9.4.3 Information not deemed private

Subscribers using the New Zealand Government PKI will be required to acknowledge that Personal Information (as defined in the Privacy Act*)* published in the certificate, primarily the name and email address of the applicant, may be used or disclosed as necessary for the efficient functioning of the PKI system.

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

The relevant CP will detail any other information that may be treated in this manner in respect of that CP.

9.4.4 Responsibility to protect private information

Information collected as part of the entities interaction with the PKI operation that is Personal Information, other than that which forms part of the *Certificate Information,* will be protected in accordance with the requirements of the Privacy Act.

Information held in the PKI can only be used by other areas within New Zealand Government where it is within the limits contained in IPP 10 of the Privacy Act. This means the information may only be used for a purpose other than the purpose for which is was collected:

i. where the entity has consented to the specific additional uses;
ii. where it is required, or authorised, by law;
iii. for the enforcement of a criminal law or a law imposing a pecuniary penalty, or for the protection of public revenue;
iv. where it is necessary to prevent or lessen a serious or imminent threat to life or health; or
v. where the use is directly related to the purposes for which the information was collected.

Given there may be a requirement to access Personal Information as part of the verification procedure, management of the access, storage, use and disclosure of information in the PKI will be in accordance with the IPPs. Access to this information is restricted to PKI *trusted roles*.

In keeping with the requirements of the Privacy Act, the PKI implements physical and logical access control mechanisms to protect the sensitive information from unauthorised access.

The New Zealand Government PKI encrypts communications of official information including the communications links between the CAs and the point of registration.

9.4.5 Notice and consent to use private information

Subscribers are to be informed of any Personal Information collected and its use and/or distribution. Refer to relevant CP for notice and consent arrangements.

9.4.6 Disclosure pursuant to judicial or administrative process

No Personal Information contained in the PKI, other than that which forms part of the Certificate Information, which relates to an identifiable New Zealand Government or subscriber entity is disclosed to any external entities to the New Zealand Government unless the disclosure is in accordance with IPP 11 of the Privacy Act. This means that information may only be disclosed:

i. where the individual is reasonably likely to have been made aware, or made aware through a privacy policy statement (which must contain particular details), that certain information is routinely passed to specific entities outside the New Zealand Government;
ii. where the individual has consented to the disclosure;

iii. where it is required by or authorised by law;
iv. for the enforcement of a criminal law or a law imposing a pecuniary penalty, or for the protection of public revenue; or
v. where it is necessary to prevent, or lessen, a serious or imminent threat to life or health.

New Zealand Government personnel and subscribers are entitled to access Personal Information about themselves in the PKI in accordance with IPP 6 of the Privacy Act. This information can be obtained by sending a signed and dated letter to the Lead Agency, requesting the relevant data. The letter is to include the person's full name, organisation and contact details, and the Lead Agency will authorise PKI staff to action the request.

Only authorised PKI staff, under two party control, are permitted to access data about individual personnel. Access by these authorised persons will be in accordance with the appropriate IPPs of the Privacy Act. The Privacy Commissioner has the right under the Privacy Act to conduct audits to ascertain whether Personal Information records are being maintained in accordance with the IPPs.

Any New Zealand Government person or subscriber is able to request changes to their own information in the PKI. Changes will, however, be subject to verification of the identity of the person requesting the change, preventing unauthorised persons from accessing or altering information.

Where changes to Personal Information (e-mail address and name) affect the contents of digital certificates, revocation and reissue of the affected certificates is required.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

Unless otherwise agreed between the relevant parties:

i. Intellectual Property Rights (IPR) in the New Zealand Government PKI Framework governance approved documents, the Certificate Directory and the CRL are owned by the New Zealand Government;
ii. IPR in the Root CAs (ECC and RCA) and AoG Shared Policy CAs (ECC and RSA) operational documentation are owned by Cogito Group, as the incumbent Service Provider;
iii. IPR in the Approved TaaS PKI Service Providers CA operational documentation are owned by the respective Service Provider;
iv. IPR in Certificates are owned by the New Zealand Government, subject to any pre-existing IPR which may exist in the Certificates or the Certificate Information;
v. the entity generating the key pairs own any IPR in the key pairs; and
vi. the Organisational Identities (OIDs) and Distinguished Names of all CAs of the New Zealand Government PKI remain the sole property of the New Zealand Government and will be allocated by the GCIO.

The IPR owners of Certificates, *Distinguished Names* and key pairs (IP Owner) grants to any other relevant entity, which has a requirement under this CPS, the CP or the other Approved Documents to use that intellectual property, the rights it reasonably requires to perform that entity's roles, functions and obligations under this CPS, the CP or the Approved Documents.

Where an entity is required under this CPS and associated CPs, or another Approved Document, to use any software or other item owned by, or licensed to, an Approved PKI Service Provider, that PKI Service Provider grants to the relevant entity any rights it reasonably requires to use that software or other item for the purposes of discharging that requirement.

The IPR owner warrants that:

i. it has all the rights necessary to grant the licences described in this 9.5; and

ii. use by relevant entities of the relevant IPR pursuant to this CPS, the CP or other Approved Documents will not infringe the IPR of a third party.

9.6 Representations and warranties

The New Zealand Government uses this CPS, associated CPs and a Subscriber Agreement to convey conditions of usage of New Zealand Government certificates to Subscribers and Relying Parties.

Participants that may make representations and warranties include New Zealand Government CAs, RAs, Subscribers, Relying Parties, and any other participants as it may become necessary.

All parties in the New Zealand Government PKI domain, including New Zealand Government CAs and RAs and Subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will promptly notify the appropriate RA.

The Lead Agency is responsible for performing the security accreditation process of the PKI core components (RCA and GNet Policy CA) with due care, in adherence to published New Zealand Government Criteria and Policies[37].

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

9.6.1 CA representations and warranties

The CA warrants:

i. the certificate information provided to it has been accurately transcribed into the certificate;
ii. all other certificate information it generates itself is accurate;
iii. the digital certificate operates with functional key pairs; and
iv. that at the time it issues a certificate the certificate contains all the elements required by the Certificate Profile as detailed in the relevant CP.

9.6.2 RA representations and warranties

The RA warrants the information in the certificate is true to the best of the RAs knowledge after performing identity authentication (registration) procedures with due diligence.

9.6.3 Subscriber representations and warranties

See relevant CP.

9.6.4 Relying party representations and warranties

Relying Parties warrant that they shall:

i. verify the validity of a digital certificate i.e. verify that the digital certificate is current and has not been revoked or suspended, in the manner specified in the CP under which the digital certificate was issued;
ii. verify that the digital certificate is being used within the limits specified in the CP under which the digital certificate was issued; and
iii. promptly notify the New Zealand Government PKI in the event that it suspects that there has been a compromise of the Subscriber's Private Keys.

9.6.5 Representations and warranties of other participants

No stipulation.

[37] Principally the PSR and NZISM, but including industry PKI specific requirements as applicable.

9.7 Disclaimers of warranties

NO IMPLIED OR EXPRESS WARRANTIES ARE GIVEN BY COGITO GROUP OR BY ANY OTHER ENTITY WHO MAY BE INVOLVED IN THE ISSUING OR MANAGING OF KEY PAIRS AND/OR CERTIFICATES ISSUED UNDER THIS CPS AND ALL STATUTORY WARRANTIES ARE TO THE FULLEST EXTENT PERMITTED BY LAW EXPRESSLY EXCLUDED.

The New Zealand Government PKI uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CPS and relevant CP. However, it gives no warranty as to their full correctness. Also, the New Zealand Government PKI cannot be held responsible for any misuse of its certificate by a Subscriber or any other party in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a Relying Party.

Any Relying Party that accepts a certificate for any usage for which it was not issued does so at its own risk and responsibility.

CA Certificates issued by Approved AoG PKI Service Providers on behalf of the New Zealand Government are primarily for internal government use and do not confer any authority, delegation or privilege independent of All of Government (AoG) or owning agency policy and procedures.

9.8 Limitations of liability

To the extent permitted by law the New Zealand Government or Cogito Group cannot be held liable for:

i. any use of certificates, other than uses specified in this CPS or the relevant CP;
ii. falsification of transactions;
iii. improper use or configuration of equipment, not operated under the responsibility of the PKI, used in transactions involving certificates;
iv. compromise of private keys associated with the certificates;
v. loss, exposure or misuse of PIN code(s) etc. protecting private keys associated with the certificates;
vi. erroneous or incomplete requests for operations on certificates;
vii. delays arising from Force Majeure; and
viii. the use of public or private keys of cross–certified (non-subordinate) CAs and their Relying Parties.

In the absence of any documented contractual relationship between the CA and a Subscriber (other than a Subscriber Agreement) and/or Relying Party, the New Zealand Government or Cogito Group does not accept any liability regarding the operations of the New Zealand Government PKI associated with certificates issued under this CPS.

Relevant contractual documents define any limitations to the extent of the liability of parties with regards to certificate use.

9.9 Indemnities

By using or accepting a certificate, each Subscriber and Relying Party agrees to indemnify and hold the New Zealand Government, as well as any of its officers, employees, agents, and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any costs or expenses of any kind, including legal fees (on a solicitor or own basis), that the New Zealand Government, as well as any of its employees, agents, and contractors may incur, that are caused by the use or publication of a certificate, and that arises from that party's:

i. misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional;

ii. violation of the Subscriber Agreement, Relying Party Agreement, this CPS, the relevant CP, or any applicable law;
iii. compromise or unauthorised use of a Certificate or Private Key caused by the negligence of that party and not by Cogito Group (unless prior to such unauthorised use the New Zealand Government has received an authenticated request to revoke the Certificate); or
iv. misuse of the Certificate or Private Key.

The Subscriber and its affiliated entities and individuals recognise that the New Zealand Government relies solely on the representations, warranties, undertakings and the information contained in the application (along with such other certificates, statements or documents as may be required or demanded by the New Zealand Government), to make a determination on recommending/not recommending the issuance of a digital certificate to the Subscriber and its affiliated entities and individuals and any misrepresentation thereof shall make the Subscriber and its affiliated entities and individuals liable, inter alia, for exemplary damages.

The indemnities contained herein shall be in addition to any other indemnities available generally in law or under the CPS or Subscriber Agreement and shall survive the termination of relationship between the Subscriber and the New Zealand Government, including as a result of suspension/revocation of the certificate.

9.10 Term and termination

9.10.1 Term

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

The CPS is available at http://www.pki.govt.nz.

9.10.2 Termination

The entire PKI may be terminated at any time by the New Zealand Government[38]. All existing certificates, expired or unexpired, revoked, or active, will be deemed unfit for further use. The New Zealand Government is not required to revoke existing certificates in this event. All CRLs may only be used for historic or evidentiary purposes upon CA termination.

The New Zealand Government is not required to give any notice to end entities before or after CA termination, however, before the New Zealand Government PKI terminates its services, it will attempt to:

i. inform entities and subordinate RAs;
ii. make widely available information of its termination; and
iii. stop issuing certificates and CRLs.

When applicable and in accordance with any external Accreditation Authority Memorandum of Agreement, the New Zealand Government will inform the external Accreditation Authority of its intention to terminate the CA and/or RA.

9.10.3 Effect of termination and survival

Unless the contrary intention appears, the expiry or termination of a contractual relationship between PKI entities which imports the terms of this CPS or a relevant CP, will not affect the continued application to those entities of any provision in this CPS or a relevant CP relating to:

[38] As per TaaS or AoG ICT Common Capabilities commercial agreements.

i. Intellectual Property Rights;
ii. Confidential Information;
iii. the protection of Personal Information;
iv. an indemnity, or
v. any other provision which expressly or by implication from its nature is intended to continue.

9.11 Individual notices and communications with participants

A notice or other communication (Notice) from one entity to another in relation to this CPS or a relevant CP requires signing by the sending entity. If the Notice delivery is electronic, it requires the sender's digital signature.

Notices to Organisations requires delivery to the physical, postal, facsimile or e-mail address of the Organisation, which is included in its Registration Information, or to another address, which the Organisation has specified to the sender.

Notices to Subscribers will be posted to the New Zealand Government PKI web page and where appropriate will be sent to the address within the certificate.

Unless otherwise specified in this CPS or a relevant CP, a Notice sent as required under this section is satisfied if:

i. it is hand-delivered to a physical address - at the time of delivery whether or not any person is there to receive it;
ii. it is posted by prepaid post - at 5pm on the third day after it is posted even if the Notice is returned to the sender;
iii. it is transmitted by facsimile - when the sending machine produces a report showing the transmission was successful;
iv. it is sent by e-mail - when it enters a system under the control of the addressee; or
v. by posting on the agreed web site - seven days after the date of posting.

If a Notice delivery occurs outside normal business hours at the addressee's place of business, the parties agree in these circumstances that formal receipt occurs at 9 am on the next *business day* at that place.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this CPS or a relevant CP are to undergo the same procedures as for the initial approval (see 1.5.4) and documented in the NZ *AoG PKI Framework Operations Manual*. Rephrasing provisions to improve their clarity as well as editorial and typographical corrections, and changes to contact details are not considered amendments. However, any change is to be brought to the attention of the Lead Agency.

9.12.2 Notification mechanism and period

The amended CPS and/or a relevant CP shall be published on the New Zealand Government PKI web site (www.pki.govt.nz) and other appropriate repositories (e.g. Public Sector Intranet) for consultation prior to it becoming effective. There is no fixed notice and comment period. Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact the parties may be changed without notice and are not subject to the notification requirements herein.

9.12.3 Circumstances under which OID must be changed

Where a CP is amended, or when a CA Certificate is renewed or replaced, the OID for the relevant CP and associated documentation must be changed (editorial changes, etc., are not considered amendments; see Sect 9.12.1,).

If a change in the New Zealand Government's CPS or CP is determined by the Lead Agency to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of this CPS will also contain a revised OID for that type of certificate.

9.13 Dispute resolution provisions

If a dispute arises between the New Zealand Government and any participating party (Dispute), written notice is to be provided so that the parties can meet to negotiate in good faith to resolve the Dispute (Dispute Notice). Where a Dispute remains unresolved 30 days after receipt of the Dispute Notice, the parties may seek mediation in accordance with the mediation rules of New Zealand. Legal representation is permissible by either party to the mediation. Each party will bear its own costs of resolving the Dispute and the parties are to bear equally the cost of any third person appointed as mediator.

Nothing in this clause prevents the New Zealand Government from preventing a party from accessing the New Zealand Government PKI, or commencing proceedings against a Subscriber for a breach of the Subscriber Agreement.

9.14 Governing law

The governance for this CPS and any relevant CP is by, and construed to be in accordance with, the laws from time to time in force in New Zealand.

The parties agree to irrevocably and unconditionally submit to the exclusive jurisdiction of the Supreme Court of New Zealand and waive any rights to object to any proceedings brought in that court.

9.15 Compliance with applicable law

All parties to this CPS and any relevant CP are to comply with all relevant:

i. New Zealand laws and regulatory requirements; and
ii. New Zealand Government information security and PKI policies.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CPS, any relevant CP and Subscriber Agreement, and TaaS commercial agreement, supersedes any prior agreements, written or oral, between the parties covered by this present document. These documents record the entire agreement between the parties in relation to its subject matter.

9.16.2 Assignment

No party may assign its obligations or rights under this CPS, or any relevant CP, without the Lead Agency's prior written approval. The Lead Agency asserts the authority of The Crown in matters relating to this CPS and the New Zealand Government PKI Framework services.

9.16.3 Severability

If any provision of this CPS and/or relevant CP is or becomes invalid, illegal or unenforceable then that provision will, so far as possible, be read down to the extent necessary to ensure that it is not illegal, invalid or unenforceable.

If the reading down of any provision, or part of the provision, is unachievable, then the provision or part of it will be void and severable, without impairing or affecting the remaining provisions of the CPS or CP (as the case may be) in any way.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Failure by either party to enforce a provision of this CPS or any relevant CP shall not be construed as in any way affecting the enforceability of that provision or the CPS or CP (as the case may be) as a whole.

9.16.5 Force Majeure

A PKI Entity is not liable for any loss or damage arising from any delay or failure to perform its obligations described in this CPS or relevant CP if such delay is due to Force Majeure. A Force Majeure event means any occurrence or omission as a result of which the party relying on it is reasonably prevented from or delayed in performing any of its obligations under this contract and that is beyond the reasonable control of that party, including, where relevant, due to forces of nature, war, riot, civil commotion, failure of a public utility, or industrial action (other than industrial action specifically directed at a party).

If a delay or failure by a PKI Entity to perform its obligations is due to Force Majeure, the performance of that Entity's obligations is suspended.

If delay or failure by a PKI Entity to perform its obligations due to Force Majeure exceeds 10 business days, the PKI Entity affected by the failure to perform the obligations may terminate the arrangement, agreement or contract it has with the non-performing PKI Entity on providing notice to that Entity in accordance with this CPS or the CP.

If the arrangement, agreement or contract terminates pursuant to this section, the non-performing PKI Entity shall refund any money (if any) paid by the terminating Entity to the non-performing Entity for services not provided by the non-performing PKI Entity.

9.17 Other provisions

No other provisions.

APPENDIX A. REFERENCES

Ref ID / Short Code	Description
ITU X.509 (2012) ISO/IEC-9594-8:2005	IT-OSI: The Directory: Public-key and attribute certificate frameworks, available at http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509
RFC 6960	RFC 6960 Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol (OCSP), Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc6960.txt
RFC 3647	RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc3647.txt
RFC 6818	RFC 6818 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force, available at http://www.ietf.org/rfc/RFC6818.txt
IETF RFC 6847	
ISO/IEC 29003	Evidence of Identity (EoI)
ISO/IEC 29115:2011	Entity Authentication Assurance Framework (EAAF)
CC EAL4 (ISO/IEC-15408:2009)	Common Criteria scheme Evaluation Assurance Level 4, available at https://www.commoncriteriaportal.org/products/, ISO/IEC-15408-x:2009 Computer Security Certification
FIPS-140-3 (ISO/IEC 19790:2012)	Federal Information Processing Standard Publication 140-3, available at http://csrc.nist.gov/groups/ST/FIPS140_3/
[CPS]	X.509 Certification Practice Statement for the New Zealand Government PKI, available at http://www.pki.govt.nz/policy/CPS.pdf
ISO/IEC 21188:2006	Public Key Infrastructure for Financial Services - Practices and Policy Framework
ISO/IEC 9594-8:2014	OSI - The Directory - Part 8: Public-key and attribute certificate frameworks, as at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64854
[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
[EoI] [LoA] [LoIP]	Levels of Assurance (LoA), and Evidence of Identity (EoI) Levels of Identity Proof (LoIP), contained in The New Zealand Government Public Key Infrastructure Core Obligations Policy document, available at http://www.pki.govt.nz
TaaS VA CP	X.509 Certificate Policy for the New Zealand Government TaaS Validation Authority Certificates, available at http://www.pki.govt.nz

NZ AoG PKI KMP	New Zealand Government TaaS Authentication Services Key Management Plan[39]
NZ AoG PKI ICTSP	New Zealand Government ICT Security Plan[40] for the New Zealand Government TaaS Authentication Services
NZISM	The New Zealand Government Information Security Manual, Version 2.5 dated July 2016, available at http://www.gcsb.govt.nz/publications/the-nz-information-security-manual/
PSR	The New Zealand Government Protective Security Requirements, available at https://www.protectivesecurity.govt.nz/
[Privacy Act]	New Zealand Privacy Act 1993, available at http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html
PRA	New Zealand Public Records Act 2005, available at http://www.legislation.govt.nz/act/public/2005/0040/latest/whole.html
IRMS	New Zealand Information and Records Management Standard and associated Archives Regulatory Framework, available at http://records.archives.govt.nz/regulatory-framework/ http://records.archives.govt.nz/resources-and-guides/information-and-records-management-standard/
TaaS	New Zealand All-of-Government 'Telecommunications as a Service' common capability.

[39] Cogito Group is the incumbent operator providing accredited management services associated with the NZ Government Root Certification Authority and TaaS Shared Policy Certificate Authority environments. Operational plans and processes for these management services remains Cogito Group intellectual property.

[40] Cogito Group document.

APPENDIX B. CERTIFICATE AUTHORITIES OPERATING UNDER THIS CPS

Service Provider Name	CA Identification (Serial)	CA Description	OID Allocated
Cogito Group	NZGovtCA001	RSA Root CA	2.16.554.101.8.1.1.2.0.1
	NZGovtCA002	ECC Root CA	2.16.554.101.8.1.1.1.0.1
	NZGovtCA201	RSA Shared Policy CA	2.16.554.101.8.1.1.2.1.1
	NZGovtCA202	ECC Shared Policy CA	2.16.554.101.8.1.1.1.1.1
	NZGovtCA203	RSA Inland Revenue Policy CA	2.16.554.101.8.1.1.2.2.1
	NZGovtCA301	RSA Cogito Shared Issuing CA	2.16.554.101.8.1.1.2.3.1
	NZGovtCA302	ECC Cogito Shared Issuing CA	2.16.554.101.8.1.1.2.2.1
	NZGovtCA303	RSA Inland Revenue Issuing CA	2.16.554.101.8.1.1.1.2.1
	NZGovtCA304	RSA MoJ (CJESP) Issuing CA	2.16.554.101.8.1.1.2.4.1
	NZGovtCA305	RSA Stats NZ Issuing CA	2.16.554.101.8.1.1.2.5.1
	NZGovtCA306	RSA MBIE GNet Issuing CA	2.16.554.101.8.1.1.2.6.1
	NZGovtCA307	RSA MVCOT Issuing CA	2.16.554.101.8.1.1.2.7.1
	NZGovtCA308	ECC Inland Revenue Issuing CA	2.16.554.101.8.1.1.2.8.1
	NZGovtCA309	ECC MPI Issuing CA	
	NZGovtCA310	ECC OT Issuing CA	
	NZGovtCA311	ECC EC Issuing CA	
	NZGovtCA312	RSA Cogito Shared Issuing CA	
	NZGovtCA313	ECC Cogito Shared Issuing CA	
	NZGovtCA314	RSA Inland Revenue Issuing CA	
	NZGovtCA315	ECC SEEMail Issuing CA	
	NZGovtCA316	RSA Stats NZ Issuing CA	
	NZGovtCA317	RSA MBIE GNet Issuing CA	
	NZGovtCA318	RSA MVCOT Issuing CA	
	NZGovtCA319	ECC Inland Revenue Issuing CA	
	NZGovtCA320	RSA DIA Issuing CA	
	NZGovtCA321	ECC OT Issuing CA	
	NZGovtCA322	ECC EC Issuing CA	
	NZGovtCA323	RSA MoJ Issuing CA	
	NZGovtCA324	ECC MPI Issuing CA	
	NZGovtCA325	ECC DIA Issuing	
Dimension Data NZ	NZGovtCA5xx	Dimension Data Shared Issuing CA	
Datacom	NZGovtCA7xx	Datacom Shared Issuing CA	

APPENDIX C. DEFINITIONS, ACRONYMS AND INTERPRETATION

C.1 Definitions

Term / Acronym	Definition or Description
Accreditation Agencies	Those agencies that provide independent assurance that the facilities, practices and procedures used to issue Cogito Group certificates comply with the relevant accreditation frameworks (policy, security and legal). Principally these will consist of DIA (in its role as Lead Agency) and GCSB (for the Root CA).
Active Directory (AD)	Microsoft product used in network and identity management. It uses the Lightweight Directory Access Protocol and typically stores information about all resources on the network. It also provides authentication services and can store PKI certificates.
Affiliated	An entity that is associated with the New Zealand Government.
Application	A computer application or relevant component of one (including any object, module, function, procedure, script, macro or piece of code)
Approved Documents	The Approved Documents are those approved by the Lead Agency and include those approved by the Accreditation Authority. E.g. CPS, CPs, ICTSP, SSP, KMP, DRBCP and Operations Manual.
AS Operator	Authentication Service Operators perform day-to-day maintenance and support of the PKI systems managed by the New Zealand Government PKI. AS Operators may also be referred to 'RA Operators' when conducting PKI certificate or key issuing and verification duties.
Authorised RA	Has the meaning given to it in paragraph 1.3.2 of this CPS.
Business Day	Any day other than a Saturday, Sunday, or New Zealand public or statutory holiday (including public service or regional holidays, where applicable). Traditionally business days operate from 0800hr to 1700hr NZT.
Card Management System (CMS)	Hardware and software applications used to manage smartcards. Smartcards are used as hard tokens for Subscribers and Operators in the New Zealand Government PKI.
CMS Auditor	Role within the CMS that has read-only access to log files for auditing purposes.
Certificate	An electronic document signed by the Certification Authority which: i. Identifies a Subscriber by way of a Distinguished Name ii. Binds the Subscriber to a Key Pair by specifying the Public Key of that Key Pair iii. Contains the information required by the Certificate Profile.
Certificate Assurance Level	See Level of Assurance.
Certificate	Information needed to generate a digital certificate as required by the

Term / Acronym	Definition or Description
Information	Certificate Profile.
Certificate Policy (CP)	Means the definition adopted by RFC3647 which defines a Certificate Policy as "A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements".
Certificate Profile	A certificate profile provides details about the format and contents of a digital certificate, including, for a natural person, their Distinguished Name. It does not use the abbreviation 'CP'.
Certificate Repository	The Certificate Repository provides a scalable mechanism to store and distribute certificates, cross-certificates and CRLs to end users of the PKI.
Certificate Revocation List (CRL)	The published directory which lists revoked Digital Certificates. The CRL may form part of the Directory or may be published separately.
Certificate Authority (CA)	A Certificate Authority (or Certification Authority) (CA) is an entity which issues digital certificates for use by other parties.
Certificate Store	Storage location for certificates on a computer or device.
Certification Practice Statement (CPS)	A CPS is a statement of the practices and procedures that a Certification Authority (CA) employs in managing the digital Certificates it issues (this includes the practices that a Registration Authority (RA) employs in conducting registration activities on behalf of that Certification Authority). These statements will describe the PKI certification framework, mechanisms supporting the application, insurance, acceptance, usage, suspension/revocation and expiration of Digital Certificates signed by the CA, and the CA's legal obligations, limitations and miscellaneous provisions. The Certificate Practice Statement (CPS) translates the Certificate Policy (CP) into operational procedures on the CA level. The CP focus is on the Certificates; the CPS focus is on the CAs.

Term / Acronym	Definition or Description
Core Components	Core components include the following: • New Zealand Government Root Certificate Authority (RCA) – self-signed root trust point of the PKI; • New Zealand Government Root Certificate Authority Operators (RCAO); • Sub Certificate Authority (Sub-CA); • Sub Certificate Authority Operators (Sub-CAO); • Registration Authority (RA); • Validation Authority (VA); • Card Management System (CMS).
Cross-certification	The establishment of a trust relationship between two PKIs, where one CA signs another PKI's CA certificate. This creates a chain of trust allowing the subscribers of the cross-certifying CA to trust those of the cross-certified CA. If done two-ways (PKIs signing each other's CAs' certificates), mutual trust can be established.
Cross-certification ceremony	The event where a cross-certification agreement is executed, i.e. one CA creates a cross-certification request to another CA. The cross-signing CA creates and returns the cross-certificate, signed with its own private key. The "ceremony" is a formal event, and is witnessed by representatives of both CAs. Details of the event are recorded and signed by the witnesses to provide an audit record.
Custodian	A person who has custody of something, a keeper or guardian; in the context of PKI, usually a *Key Custodian.*
New Zealand Government **Information Environment**	The New Zealand Government Information Environment encompasses the computing and communications infrastructure of the New Zealand Government along with the management systems and people that deliver that infrastructure.
New Zealand Government **Root CA (RCA)**	A New Zealand Government operated CA that provides a self-signed certification authority (CA) certificate that identifies a CA and provides the trust chain anchor for the NZ Government PKI Framework. (A CA can issue multiple certificates, which can be used to issue multiple certificates in turn, thus creating a tree).
Device	Device means any computer hardware or other electronic device.
Digital Signature	An electronic signature created using a Private Signing Key.
Directory Service	A directory service is a software application – or a set of applications – that stores and organises information about a computer network's users and network resources, and that allows network administrators to manage users' access to the resources. Additionally, directory services act as an abstraction layer between users and shared resources. The LDAP directory services are examples of general-purpose distributed hierarchical object-oriented directory technologies. Both offer complex searching and browsing capabilities are used for white pages, network information services, PKI, and a wide range of other applications.
Distinguished Name (DN)	An unique identifier assigned to, as relevant: i. the Subscriber identified by; and

Term / Acronym	Definition or Description
	ii. the issuer of a Certificate, having the structure required by the Certificate Profile
Evaluation Assurance Level (EAL)	The Evaluation Assurance Level (EAL1 through EAL7) of a computer product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The increasing assurance levels reflect added assurance requirements that are to be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented.
Evidence Of Identity (EoI)	Evidence (e.g. in the form of documents) issued to substantiate the identity of the presenting party, usually produced at the time of Registration (i.e. when authentication credentials are issued).
Exercised	To discharge, or perform, a function. Or, an act of employing or putting into play.
Hard Token	A hard token, sometimes called an "authentication token," is a hardware security device that is used to authorise a Subscriber. A common example of a hard token is a smartcard.
High Assurance (HA)	A category defined by the Accreditation Authority that requires CAs and RAs meet the standards as set out in PSR and ISM and for certificates to be issued on the basis of the Formal Identity Verification Model and be able to be relied up on by multiple Government agencies.
High Assurance Certificate	A digital certificate issued by an Accredited or Recognised Service Provider to Organisations and individuals for the purpose of transacting online with government agencies and whose risk and threat to data are assessed as high. This category is characterised by a requirement for a Formal Identity Verification Model *EOI* check by an accredited Registration Authority.
Identity Certificate	An identity certificate is a certificate which uses a digital signature to bind together a public key with a human identity — information such as the name of a person, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Key	A Key is a string of characters used with a cryptographic algorithm to encrypt and decrypt.
Key Custodian	A key custodian refers to the authorised person appointed to manage a key on behalf of the New Zealand Government.
Key Pair	A pair of asymmetric cryptographic Keys (e.g. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key.
Level of Assurance (LoA)	Levels of trust associated with a credential as measured by the associated technology, processes, and policy and practice statements controlling the operational environment. In the context of this CPS, the term refers to four levels of assurance of certificates (low, medium, high, very high) defined for the New Zealand Government PKI.

Term / Acronym	Definition or Description
Network Resource	Network Resources (devices) are units that mediate data in a computer network. Computer networking devices are also called network equipment and commonly include routers, gateways, switches, hubs, repeaters and firewalls.
Non-Person Entity	An entity with a digital identity (for example an IP address or MAC address) that acts in cyberspace, but is not a legal entity. This can include web sites, hardware devices, software applications, and information artefacts.
M-of-N (also 'm-of-n')	M of N control is a policy of dividing up a task among multiple entities so that no one person acting alone can perform the entire task. It is used to help minimize an organization's exposure to the risk of one person misusing a privilege, and performing a sensitive action like key recovery without authorization. M of N keys provide additional security by requiring a predefined number of people (M) out of a group of people (N) be present with individual tokens, before the private key stored on the secure cryptographic token can be accessed, thus decreasing the risk of collusion between operators.
Modification (of certificate)	Certificate modification means the issuance of a new certificate due to changes in the information in the certificate other than the Subscriber public key. (RFC3647)
Object IDentifier (OID)	An OID is a string of decimal numbers that uniquely identifies an object. These objects are typically an object class or an attribute. It serves to name almost every object type in X.509 Certificates, such as components of Distinguished Names and Certificate Policies. See http://www.oid-info.com/.
Online Certificate Status Protocol (OCSP)	Method of establishing the status of a certificate that has not expired. A PKI enabled client requests the status of a certificate from an OCSP responder. The responder provides a response ("good", "revoked" or "unknown") to the client. OCSP is a more bandwidth efficient method than the download of a full Certificate Revocation List (CRL).
Operational Day	Any day that the PKI facility is manned. In this context it normally occurs in conjunction with a *Business Day*.
Peer PKI	Other PKI which the New Zealand Government PKI has entered (or intends to enter) into a cross-certification arrangement with.
Personal Identity Verification (PIV)	Standard created by National Institute for Standards and Technology (NIST) in response to Homeland Security Presidential Directive 12 (HSPD 12) of Aug 2004. Full name "Personal Identity Verification of Federal Employees and Contractors". Also known as FIPS 201. Specifies interfaces, biometrics and algorithms for PIV compliant cards.
Operations Manager	Manages PKI and Identity Brokerage operations within the New Zealand Government Authentication Services.
Private Certificate-Signing Key	The Private Key used by the CA to digitally sign Certificates.

Term / Acronym	Definition or Description
Private Confidentiality Key	The Key used by the addressee to decrypt messages, which have been encrypted using the corresponding Public Confidentiality Key.
Private Key	The Private Key in asymmetric Key Pair that must be kept secure to ensure confidentiality, integrity, authenticity and non-repudiation, as the case may be.
Private Signing Key	A Private Key used to digitally sign messages on behalf of the relevant Subscriber.
Public Key	The Key in an asymmetric Key Pair which may be made public.
Public Key Infrastructure (PKI)	The combination of hardware, software, people, policies and procedures needed to create, manage, store and distribute Keys and Certificates based on public key cryptography.
PKI Disclosure Statement (PDS)	A PDS is a supplementary document that aims to provide a concise, 'clear and conspicuous' framework to disclose and emphasise critical information about the policies and procedures of a certificate authority that is addressed in much greater detail in the Certificate Policy Statement (CPS) and associated Certificate Policies (CPs), which in turn demonstrate compliance with the New Zealand Government PKI Framework Core Obligations Policy.
PKI Software	Software programs that manage digital certificate lifecycle operations and token management.
Public Key Technology (PKT)	Public Key Technology is the hardware and software used for encryption, signing, verification as well as the software for managing Digital Certificates.
Registration Authority (RA)	A Registration Authority (RA) is an entity that is responsible for one or more of the following functions on behalf of a CA: i. processing certificate application; ii. processing requests to revoke certificates, and iii. processing requests to renew, re-key or modify certificates. Processing includes the identification and authentication of certificate applicants and approval or rejection of requests. See section 1.3.2 (Registration Authorities) of this CPS and the relevant Certificate Policy (CP) for more information about the applicable RA.
RA Operator (RAO)	A uniquely approved and trusted individual that acts as the Operator for a RA. Holds privileged user access rights to the RA terminal and associated CA certificate/CRL server. The RA is responsible for maintaining the quality of PKI Certificate or Key issuing services, including verifying requests and certificate details, and record keeping.
Registration Officer (RO)	A person authorised by a New Zealand Government Registration Authority (RA) or New Zealand Government approved "Third party" RA to perform RA functions in accordance with this CPS, the relevant Certificate Policy and other applicable documentation.
Re-Key	A Subscriber or other participant generating a new key pair and applying

Term / Acronym	Definition or Description
	for the issuance of a new certificate that certifies the new public key. Normally used at the time of expiry of the certificate. (RFC3647)
Relying Party	A recipient of a Certificate who acts in reliance on that Certificate and/or Digital Signatures verified using that Certificate.
Renewal (of certificate)	Renewal means the issuance of a new certificate to the Subscriber without changing the Subscriber's public key or any other information in the certificate. (RFC3647). The validity period and serial number will be different in the renewed certificate.
Repository	A database of information (e.g. Certificate status, evaluated documents) which is made accessible to users including the Relying Parties.
Resource	Includes any Network Resource, *Application*, code, electronic service or process, *Device,* or data object that is capable of utilising a Certificate.
Resource Certificate	A Resource Certificate is a Certificate issued in respect of a Resource.
Revoke	To terminate a Certificate prior to the end of its operational period.
Root CA (RCA)	A CA that is at the top of a certificate chain, i.e. its own certificate is self-signed.
Secure Sockets Layer	A protocol developed by Netscape for transmitting private documents via the Internet.
Subordinate CA (Sub-CA)	A CA which is has been established under the certificate path of the New Zealand Government Root CA (RCA). A Sub-CA usually issues and manages certificates to end entities. Includes both Policy and Issuing CAs.
Subscriber	A Subscriber is, in the context of this CP: i. the entity whose Distinguished Name appears as the "Subject Distinguished Name" on the relevant Certificate, and / or ii. the person or legal entity that applied for that Certificate, and / or entered into the Subscriber Agreement in respect of that Certificate.
Subscriber Agreement	An agreement between the relevant Service Provider and a Subscriber, which sets out the respective rights, obligations and liabilities of those parties, and which legally binds those parties to the relevant Certificate Policy and Certification Practice Statement. In context of the NZ AoG PKI Framework, the TaaS 'PKI Subscription Form' and confirmation that both parties are complying with the 'AoG PKI Core Obligations' policy (or relevant PDS), equate to meeting the requirements of a PKI 'Subscriber Agreement'.
Subscriber Authority (SA)	
Telecommunications as a Service (TaaS)	An AoG ICT Common Capability, managed by the Department of Internal Affairs (DIA) on behalf of the Government Chief Information Officer (GCIO).
Token	A hardware security device containing a user's Private Key(s), and Public

Term / Acronym	Definition or Description
	Key Certificate.
Transport Layer Security (TLS)	A cryptographic protocol that provides security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end.
Trusted Role	A role conducted within a RA/CA that has access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Certificates, including operations that restrict access to a repository. Personnel who perform this role are qualified to serve in it.
Validation Authority (VA)	A Validation Authority (VA) is an entity that can perform one or more of the following functions: i. processing certificate status requests; ii. validating credentials and authentication requests; iii. validating signatures; and iv. other services related to PKI and online authentication. The Cogito Group Validation Authority provides certificate status information through the provision of OCSP responders, and may expand its services in the future to include Server-based Certificate Validation Protocol (SCVP) services.
X.509 and X.509v3	The international standard for the framework for Public Key Certificates and attribute Certificates. It is part of wider group protocols from the International Telecommunication Union-T X500 Directory Services Standards.

C.2 Acronyms

AD Active Directory

AoG All of Government

BOC Backup Operations Centre

CA Certification Authority

CAL Certificate Assurance Level

CAO CA Operator

CCA Cross-Certification Arrangement

CMS Card Management System

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSA Certificate Status Authority – equivalent to Validation Authority (VA), found in ACP185

DN Distinguished Name

DRBCP	Disaster Recovery and Business Continuity Plan
RCA	Root Certificate Authority
RCAO	Root Certificate Authority Operator
EAL	Evaluated Assurance Level
EOI	Evidence of Identity
EPL	Evaluated Products List
HSM	Hardware Security Module
ICTSP	Information Communication Technology Security Plan
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Intellectual Property
IPR	Intellectual Property Rights
ISM	New Zealand Government Information Security Manual
ISO	International Standards Organisation
ITSEC	Information Technology Security Evaluation Criteria
KMP	Key Management Plan
LOA	Level of Assurance
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PIV	Personal Identification Verification
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PKT	Public Key Technology
POC	Primary Operations Centre
RA	Registration Authority
RAO	Registration Authority Operator
RFC	Request For Comment
RO	Registration Officer
SA	Subscriber Agreement (TaaS Subscription Form)
SCVP	Server-based Certificate Validation Protocol
SO	Security Officer
SRMP	Security Risk Management Plan
SSL	Secure Sockets Layer
SSP	System Security Plan

Sub-CA	Subordinate Certificate Authority (Policy and Issuing)
Sub-CAO	Subordinate Certificate Authority Operator
TaaS	Telecommunications as a Service
TLS	Transport Layer Security
UPS	Uninterruptible Power Supplier
URI	Uniform Resource Identifier
VA	Validation Authority

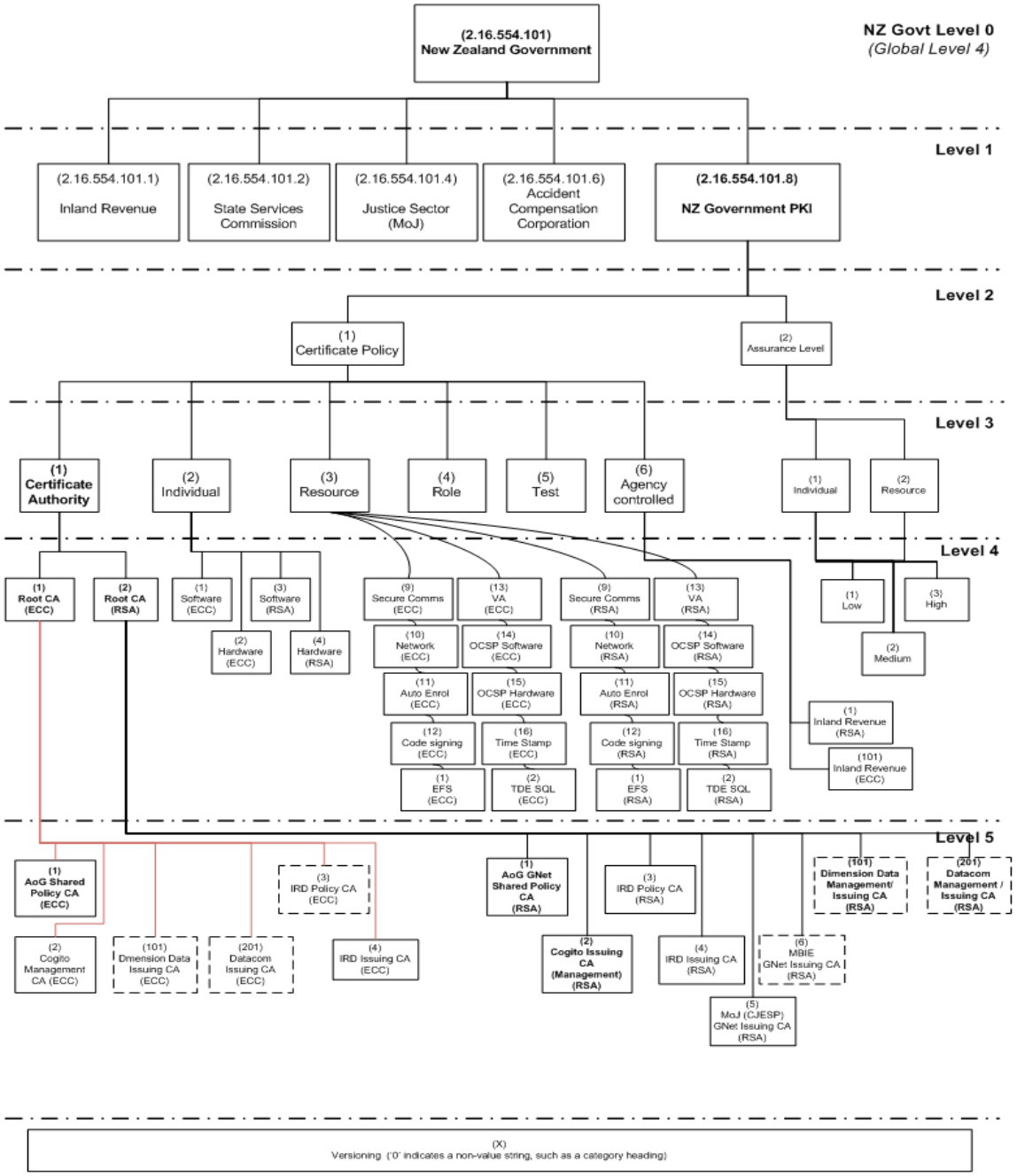
C.3 Interpretation

In Approved Documents, unless the contrary intention appears:

i. a reference to the singular includes plural and vice versa;
ii. words importing a gender include any other gender;
iii. a reference to a person includes a natural person, partnership, body corporate, association, governmental or local authority or agency, or Device or Application or other entity;
iv. a reference to a document or instrument includes the document or instrument as altered, amended, supplemented or replaced from time to time;
v. a reference to a section is a reference to the relevant section of that document;
vi. an amendment or replacement of a document does not imply any consequent amendment or alteration to any other document;
vii. where a word or phrase is given a particular meaning, other parts of speech and grammatical forms of that word or phrase have corresponding meanings;
viii. the meaning of general words is not limited by specific examples introduced by 'including', 'for example' or similar expressions;
ix. the headings are for convenience only and are not to be used in the interpretation of an Approved Document; and
x. any appendix or attachment to an Approved Document (no matter how named) forms part of that document.

APPENDIX D. NZ GOVERNMENT PKI FRAMEWORK – OBJECT IDENTIFIER (OID) STRUCTURE

DETAILED NEW ZEALAND GOVERNMENT OID TREE



Version 1.2.1 – Proposed, April 2017

Author: Phil Cutforth (AoG EA), DIA

APPENDIX E. APPROVED CERTIFICATE POLICIES

OID reference	CP Title	POC
2.16.554.101.8.1.1.1.0.1	X.509 Certificate Policy for the New Zealand Government **Root Certification Authority (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.1.2.0.1	X.509 Certificate Policy for the New Zealand Government **Root Certification Authority (RSA/ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.1.1.1.1	X.509 Certificate Policy for New Zealand Government **Shared Policy (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.1.2.1.1	X.509 Certificate Policy for New Zealand Government **Shared Policy (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.1.1.2.1	X.509 Certificate Policy For New Zealand Government **Issuing (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.1.2.2.1	X.509 Certificate Policy For New Zealand Government **Issuing (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.2.1.0.1	X.509 Certificate Policy For New Zealand Government **Individual Software (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.2.2.0.1	X.509 Certificate Policy For New Zealand Government **Individual Hardware (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.2.3.0.1	X.509 Certificate Policy For New Zealand Government **Individual Software (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.2.4.0.1	X.509 Certificate Policy For New Zealand Government **Individual Hardware (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.1.0.1	X.509 Certificate Policy for New Zealand Government **Secure Communications Certificates (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.2.0.1	X.509 Certificate Policy for New Zealand Government **Network Resource Certificates (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.3.0.1	X.509 Certificate Policy for New Zealand Government **Auto-enrol Resource Certificates (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz

OID reference	CP Title	POC
2.16.554.101.8.1.3.4.0.1	X.509 Certificate Policy for New Zealand Government **Code-Signing Resource Certificates (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.5.0.1	X.509 Certificate Policy for New Zealand Government **Validation Authority Certificates (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.6.0.1	X.509 Certificate Policy for New Zealand Government **OCSP Software (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.7.0.1	X.509 Certificate Policy for New Zealand Government **OCSP Hardware (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.8.0.1	X.509 Certificate Policy for New Zealand Government **Timestamp Authority Certificates (ECC)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.9.0.1	X.509 Certificate Policy for New Zealand Government **Secure Communications Certificates (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.10.0.1	X.509 Certificate Policy for New Zealand Government **Network Resource Certificates (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.11.0.1	X.509 Certificate Policy for New Zealand Government **Auto-enrol Resource Certificates (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.12.0.1	X.509 Certificate Policy for New Zealand Government **Code-Signing Resource Certificates (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.13.0.1	X.509 Certificate Policy for New Zealand Government **Validation Authority Certificates (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.14.0.1	X.509 Certificate Policy for New Zealand Government **OCSP Software (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.15.0.1	X.509 Certificate Policy for New Zealand Government **OCSP Hardware (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz
2.16.554.101.8.1.3.16.0.1	X.509 Certificate Policy for New Zealand Government **Timestamp Authority Certificates (RSA)**	Cogito Group authentication.services@cogitogroup.co.nz