

PKI Disclosure Statement

for the

New Zealand Government PKI

RSA Individual - Software Certificates

(Medium Assurance)

Version 0.3

May-16

Notice to all parties seeking to rely

Reliance on a Certificate issued in association with this PKI Disclosure Statement (PDS), you must have read and understood the provisions of this document. Further information can be found under the Certificate Policy, identified by sub arcs of the object identifier **2.16.554.101.8.1.2.3.0.1** and the New Zealand Government PKI Framework Core Obligations Policy. Use of this document and associated certificates constitutes acceptance of the terms and conditions set out.

The acceptance of a certificate by a Relying Party for a prohibited purpose is at the Relying Party’s risk. Engaging in a prohibited Certificate use is a breach of this PKI Disclosure Statement and associated Certificate Policy and the New Zealand Government disclaims any and all liability in such circumstances. The conditions applicable to each type of New Zealand Government Certificate will vary.

**Document Management**

|  |  |
| --- | --- |
| **Controlled and Maintained by:** | Cogito Group |
| **Approved and Changes authorised by:** | Lead Agency (DIA) |

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Issue Date** | **Description/ Amendment** | **Changed by** |
| 0.1 Draft | Apr 2016 | Initial draft. | SJL |
| 0.2 | Apr 2016 | GCIO Review | PC |
| 0.3 | May 2016 | Updates from GCIO Review | SJL |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Signatures**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Organisation** | **Name, Appointment** | **Signature** |
| Operations Manager | Cogito Group |  |  |
| Lead Agency SRO | DIA (Lead Agency) |  |  |

**References**

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Version** | **Issue Date** | **Title / Description** |
| NZISM | v2.4 | Nov 2015 | NZ Information Security Manual |
| 2.16.554.101.8.1.2.3.0.1 | v1.0 | Apr 2016 | NZ Govt PKI Individual – Software (Medium Assurance) (ID-MAC) Certificate Policy (CP) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

1. Introduction 4

2. Certificate Authority and Registration Authority Contact Information 4

2.1 Certificate Authority and Registration Authority 4

3. Certificate Description 4

3.1 Certificate Type 4

3.2 Certificate Usage 5

3.2.1 Appropriate certificate uses 5

3.2.2 Prohibited certificate uses 5

3.3 Certificate Validity Period 6

3.4 Validation Procedures 6

4. Reliance Limits 7

5. Obligations of Subscribers 7

6. Obligations of Relying Parties 7

7. Warranties, liabaility and Indemnities 8

7.1 Limited Warranty 8

7.1.1 CA representations and warranties 8

7.1.2 RA representations and warranties 9

7.2 Disclaimer 10

7.3 Limitation of Liability 10

7.4 Indemnities 10

8. Applicable agreements, Certification Practice Statement, Certificate Policy 11

8.1 Applicable Agreements 11

8.2 Certification Practice Statement (CPS) 11

8.3 Certificate Policy (CP) 12

9. Privacy 12

9.1 Privacy Policy 12

9.2 Privacy plan 12

9.3 Information treated as private 12

9.4 Information not deemed private 12

9.5 Responsibility to protect private information 13

9.6 Notice and consent to use private information 13

9.7 Disclosure pursuant to judicial or administrative process 13

10. Refund Policy 13

11. Applicable Law 13

12. Dispute Resolution 14

13. Audit 14

13.1 Frequency of Audit 14

14. Trust Marks 15

# Introduction

*Public Key Infrastructure* (PKI) *Disclosure Statements* (PDS) are a supplementary document that aim 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 associated *Certificate Policies* (CPs) and the *Certificate Policy Statement* (CPS), which in turn demonstrate compliance with the New Zealand Government PKI Framework Core Obligations Policy.

A PDS does not substitute a fully detailed CP, a PDS functions as a substitute for a large CP in limited situations, for example, when a relying party needs to decide quickly if it will rely on a previously unfamiliar CA’s certificates assisting them in making informed trust decisions.

This PDS provides an overview of the rules to manage the New Zealand Government PKI *Individual – Software (Medium Assurance)* (ID-MAC) identity certificates, including an overview of the obligations of the Public Key Infrastructure (PKI) entities, and how the parties, indicated below, use them. It does not describe how to implement these rules as that information is in the CPS, or documents referenced by the CPS. In general, the rules identify the minimum standards in terms of performance, security and/or quality.

The headings in this PDS follow the framework set out in the American Bar Association (ABA) PKI Assessment Guidelines.

# Certificate Authority and Registration Authority Contact Information

Cogito Group Limited provide this service on behalf of New Zealand Government for use by Public Sector entities, principally but not exclusively, in support of the Telecommunications as a Service (TaaS) Government Network (GNet) services.

## Certificate Authority and Registration Authority

Cogito Group

PO Box 5398

Lambton Quay

Wellington 6145

Telephone: +64 22 694 2169

Email: [authentication.services@cogitogroup.com.au](mailto:authentication.services@cogitogroup.com.au)

# Certificate Description

## Certificate Type

An ID-MAC is used to identify an individual who has an affiliation with the New Zealand Government (Staff, Subscriber Organisation, Contractor or Consultant etc.) and who has a requirement, which has been approved by the New Zealand Government, to:

1. Interact directly with New Zealand Government assets or systems, using *Public Key Technology* (PKT);
2. Authenticate with a third party, as an affiliate of the New Zealand Government or customer organisation; or
3. Provide a *digital signature*, as an individual *affiliated* with the New Zealand Government or subscriber organisation.

There are two types of certificates issued under this CP, namely:

1. Signing/authentication certificates; and
2. Encryption/confidentiality certificates.

No authority, or privilege, applies to an individual by becoming an approved ID-MAC holder, other than confirming an affiliation with the organisation.

The CP for this certificate allows *Subscribers*’ *keys* and certificates to reside on soft or hardware based *tokens*.

Note that this PDS does not preclude Subscribing Agencies having more than one ID-MAC PDS in their PKI structure; such as for permanent staff from contractors and other temporary staff. Supplementary ID-MAC PDS must be based on this overarching PDS and must comply with the same reference sources in order to be considered under the New Zealand Government PKI Framework. The Subscribing Agency would be responsible for the production and approval of such agency-specific PDS.

## Certificate Usage

Certificates issued under this PDS, in conjunction with their associated private keys, allow a Subscriber to:

1. Authenticate themselves to a Relying Party electronically in online transactions;
2. Digitally sign electronic documents, transactions and communications; and
3. Confidentially communicate with a Relying Party.

The certificate policies extension will be used to clearly indicate the object identifier (OID) under which the Certificate has been issued and the purposes for which the Certificate may be used.

### Appropriate certificate uses

Certificates issued under this PDS, in conjunction with their associated private key, may be used:

1. For the authentication of the identity of a Subscriber, during the conduct of any lawful business with that individual, as an individual affiliated with the New Zealand Government and for which the *level of assurance* has been assessed as sufficient by the Lead Agency and the Relying Party organisation;
2. To provide accountability and non-repudiation of ID-MAC Subscriber transactions or communications;
3. To verify the integrity of a communication from a Subscriber to a Relying Party; and
4. For the sending and receiving of confidential communications, provided such communication is in accordance with normal New Zealand Government business and security policy and procedures.

### Prohibited certificate uses

The prohibited uses for certificates issued under this CP are:

1. To use the certificate in a way that represents that the certificate possesses any attribute, authority, access, privilege or delegations that may be afforded to the Subscriber.
2. To use the certificate in a way that represents that communications and transactions can only occur over certain specified infrastructure for that transaction or communication.
3. For a Subscriber to conduct any transaction, or communication, which is any or all of the following:
   1. Unrelated to organisational business;
   2. Illegal and/or criminal;
   3. Unauthorised;
   4. Unethical, or
   5. Contrary to New Zealand Government regulatory frameworks.

The acceptance of a certificate by a Relying Party for a prohibited purpose is at the Relying Party’s risk. Engaging in a prohibited certificate use is a breach of the responsibilities and obligations agreed to by the Subscriber and the New Zealand Government disclaims any and all liability in such circumstances.

## Certificate Validity Period

ID-MAC identity Certificates are valid for no more than two years, where they are manually enrolled; or no longer than one year for Certificates that are automatically enrolled (auto-enrollment).

## Validation Procedures

ID-MAC Certificates must be validated using X.509 Certificate processing rules.

Subscribing Agencies must conduct Evidence of Identity (EoI)[[1]](#footnote-1) assessment and approval for requested Subscriber Certificates. It is also expected that Subscribing Agencies would require all individuals to sign the equivalent of a Certificate Holder Agreement[[2]](#footnote-2). No Subscriber should be able to authorize production of their own Certificate, and all Certificate Requests must be authorized by the agencies Subscriber Authority (as defined in the CPS).

Applicants must have an account within the Subscriber organisation Information Environment (IE), thus the affiliation with the organisation is validated.

The creation of a network account initiates the Certificate issuance.

A soft token containing the *key pair* is generated for the individual on the workstation the first time the user logs in to their account. To prove possession of the private key, a digitally-signed Certificate Request is submitted to the RA. The submission is made using the credentials supporting access to the individuals account within theIE.

Certificates should normally be automatically renewed for all users. If reissue is necessary, the same procedure is followed as for initial issue.

Subscribing Agencies may have additional procedures to follow to authorize Certificate issue, though these will be in addition, not in replacement, of the above.

# Reliance Limits

ID-MAC Certificates issued by Cogito Group 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 agency policy and procedures.

# Obligations of Subscribers

As the authorized Certificate holder, the Subscriber, in obtaining access to the network, acknowledges that the information provided by them is true to the best of their knowledge.

In addition, Subscribers MUST:

1. only use Keys and digital certificates within the limits specified in the CP;
2. take all reasonable measures to protect their Private Key(s) from compromise, and take all necessary precautions to prevent loss, disclosure, modification, or unauthorised use of their Private Key(s);
3. take all reasonable measures to protect; and accept responsibility for; the security, safety, confidentiality and integrity of relevant passwords, passphrases and PINs associated with the issued Keys and digital certificates from disclosure at all times;
4. take all reasonable measures to protect any device, token or other physical media that contains their Keys and digital certificates, including all necessary precautions to prevent loss, intentional damage, disclosure, modification, or unauthorised use of such;
5. promptly notify the RA (usually through their Subscribers Authority) in the event that they consider or suspect there has been a compromise of their Private Key(s); and
6. promptly notify the RA in the event that they consider the EOI, or any other information provided by them, is or may be incorrect;
7. promptly notify the Subscribers Authority in the event that any information provided by them in context of the Certificate Holders (Subscribers) Agreement;
8. accept sole responsibility for the contents of any transmission, message, or other document/data signed using their Keys or digital certificates[[3]](#footnote-3); and
9. promptly return physical media containing Keys and digital certificates to the Subscribers Authority upon request or cessation of employment by the Subscribing Agency.

Subscribers MUST NOT:

1. disclose their passwords; or
2. share media containing their Keys or digital certificates with anyone else (including privileged users, such as system administrators).

A Subscriber may hold more than one Identity Certificate (such as one for authentication and non-repudiation purposes; and separately one for data encryption).

# Obligations of Relying Parties

Before relying on the Subscriber certificate, a Relying Party must:

1. verify the validity of a digital certificate;
2. verify that the digital certificate is being used within the limits specified in the CP;
3. verify the entire certificate chain up to the AoG Root CA (where appropriate), or Policy / Issuing CA as the highest authority, prior to relying on the Certificate; and
4. promptly notify the RA in the event that it suspects that there has been a compromise of the Subscriber’s *Private Keys[[4]](#footnote-4)*.

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

1. The processes of checking validity of the Subscriber’s certificate;
2. Any authority, or privilege, of the Subscriber to act on behalf of the New Zealand Government; and
3. Any authority, access or privilege the Subscriber has to the Relying Party’s assets or systems.

A Relying Party agrees to the conditions of this PDS, the associated CP and the CPS. The use of a certificate, or associated revocation information, issued under this PDS is the Relying Party’s acceptance of the terms and conditions of this PDS, relevant CP and CPS.

# Warranties, liabaility and Indemnities

## Limited Warranty

The New Zealand Government uses this PDS, the CPS and associated CPs and a Subscriber Agreement (SA) 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.

In particular, Cogito Group and the New Zealand Government (Lead Agency) warrants that Certificate holders (Subscribers) private signing Keys used for non-repudiation are not escrowed or otherwise copied. The only copy of the private signing Key is the one held by the Subscriber.

### CA representations and warranties

The CA warrants:

1. the certificate information provided to it has been accurately transcribed into the certificate;
2. all other certificate information it generates itself is accurate;
3. the digital certificate operates with functional key pairs; and
4. 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;
5. all CA staff hold appropriate security clearances and are suitably trained for their role;
6. all staff operating the ID-MAC[[5]](#footnote-5) CA have been identified to a ‘High’ level of identity proofing (i.e. LoIP 3);
7. provide a process for Subscribers and Subscriber Authorities; and Lead Agency in an emergency; to request revocation of their own certificates;
8. provide a process for Lead Agency to request revocation of all Subscribing Agency and CA certificates in an emergency[[6]](#footnote-6);
9. the CA/RA will revoke Subscriber certificates promptly, where it is made aware or obtains evidence that a Subscribers certificate has been compromised or falsely acquired;
10. revocation of certificates will be published to the CRL in a timely manner, in accordance with the timelines CA and RA Operation Manuals; and in a manner compliant with the CPS;
11. all PKI components (including facilities) comply with the CP and CPS assurance requirements; and
12. the CA will operate and maintain a CRL, and where supported OCSP capabilities, in accordance with the CPS and respective CP(s);
13. the CA will not archive Keys used for digital signature, authentication, or non-repudiation;
14. the CA will maintain log records of all operations, including the RA; and in particular be able to uniquely identify any instance of key recovery from logs, in accordance with the CPS requirements;
15. the CA will maintain an AoG Accreditation status in accordance with the GCIO and Lead Agency process and requirements, including annual audits; and
16. in the event of CA termination, the CA:
    1. will not enter into new Subscriber Agreements or contracts, or renew existing arrangements;
    2. will notify the Lead Agency and all Subscribing Agencies (via agency nominated Subscriber Authority) to provide a minimum notification period of 24hrs.; and
    3. will make arrangements to novate existing PKI services and certificates to an alternative NZ Govt PKIF (TaaS) approved service provider, or to the Subscribing Agency itself; or to gracefully terminate all Subscriber Agreements that were entered into, in accordance with the relevant CP(s);
    4. co-operate with the Lead Agency and other Service Providers in termination of the CA services.

### RA representations and warranties

The RA warrants that:

1. the information in all Subscriber’s certificates is true to the best of the RAs knowledge; after performing identity authentication (registration) procedures with due diligence;
2. the RA will protect all Subscriber personal information in accordance with the Privacy Act 1993;
3. in the event that an error is identified in the identity proofing process that gives rise to uncertainty as to the identity of a Subscriber, they will promptly notify the relevant CA and request revocation where necessary; and
4. will not conduct Key recovery or renewal on any Subscribers certificates without prior authorisation by the CA and Subscriber Authority.

## Disclaimer

The New Zealand Government PKI Framework uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by the CPS and relevant CP. However, it gives no implied or express warranty as to their full correctness. Also, the New Zealand Government PKI Framework 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.

## Limitation of Liability

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

1. any use of certificates, other than uses specified in the CPS or the relevant CP;
2. falsification of transactions, including Subscriber identity proofing;
3. improper use or configuration of equipment, not operated under the responsibility of the PKI, used in transactions involving certificates;
4. compromise of private keys associated with the certificates;
5. loss, exposure or misuse of PIN code(s) etc. protecting private keys associated with the certificates;
6. erroneous or incomplete requests for operations on certificates;
7. delays arising from Force Majeure; and
8. 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 Framework associated with certificates issued under the CPS.

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

## 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:

1. misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional;
2. violation of the Subscriber Agreement, Relying Party Agreement, this CPS, the relevant CP, or any applicable law;
3. 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
4. illegal and improper 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.

# Applicable agreements, Certification Practice Statement, Certificate Policy

## Applicable Agreements

A Subscriber or Relying Party agrees to the conditions of this PDS, the CP and CPS. The use of a certificate, or associated revocation information, issued under the CP is the Subscriber and Relying Party’s acceptance of the terms and conditions of this PDS, the CP and CPS.

This PDS generally follows the format suggested by the American Bar Association (ABA) in their PKI Assessment Guidelines.

## Certification Practice Statement (CPS)

This PDS is associated with the New Zealand Government PKI CPS. The purpose of the CPS is to provide a common framework under which the New Zealand Government PKI, CA and RA, services are provided. As such, it describes the practices Cogito Group employs in issuing digital certificates on behalf of the New Zealand Government. 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 PKI certificates.

The CPS adheres to the standard set out in the Internet Engineering Taskforce (IETF) RFC 3647, and is complemented by a series of PDS documents, each of which promulgates the rules applying to a particular class of certificates issued by Cogito Group on behalf of the New Zealand Government.

This CPS should be read in conjunction with the relevant CP(s), which set 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.

The CPS states how the New Zealand Government PKI Framework Core Obligations Policy requirements will be maintained.

The relevant version of the CPS is published at [www.pki.govt.nz/policy/](http://www.pki.govt.nz/policy/).

## Certificate Policy (CP)

This PDS functions as a summary of the associated CP, by stating the rules applying to the use of ID-MAC Certificates and defining their community of use.

This PDS is associated with the Medium assurance X.509 Certificate Policy (CP) for the New Zealand Government Individual Identity Software for the RSA algorithm family, which carries the OID 2.16.554.101.8.1.2.3.0.1. The CP identifies the rules to manage the New Zealand Government PKI Individual – Software (Medium Assurance) identity (ID-MAC) certificates, including the obligations of the PKI entities, and how the parties use them.

The ID-MAC CP is one of a family of CP’s related to the PKI framework and CPS. The relevant version of the CP is published at [www.pki.govt.nz/policy/](http://www.pki.govt.nz/policy/).

# Privacy

## Privacy Policy

In order to provide an audit and evidentiary trail of the verification process, and documentation presented to confirm an individual’s identity, The New Zealand Government is required to collect Personal Information as defined in the Privacy Act 1993 [Privacy Act]. The collection, use and disclosure of such information is governed by the Privacy Act.

At enrolment, applicants acknowledge that the New Zealand Government may collect, use or disclose Personal Information about them.

The New Zealand Government PKI Framework Privacy Statement is available at [www.pki.govt.nz/policy/](http://www.pki.govt.nz/policy/).

Personal information gathered by Cogito Group on behalf of the New Zealand Government for the purpose of issuing Keys and Certificates will be gathered and stored in accordance with the Privacy Act. All subscribers are advised that the information contained in and pursuant to this PDS and the associated CPS, and supporting documents, is Official Information in terms of the Official Information Act 1982; and in line with the policy of that Act, such information may be released unless there is a good reason in terms of that Act to withhold the information.

## Privacy plan

Cogito Group must not disclose personal information of Certificate Holders without their prior consent unless required by law. The Privacy Act and Privacy Principles form the basis for the New Zealand Government PKI Framework privacy plan.

## Information treated as private

Personal information held by Cogito Group but not appearing in certificates or public directories is considered private and shall not be disclosed by Cogito Group.

## Information not deemed private

Personal information that is publicly available, appearing in certificates and in public directories, is not considered private. This may include a CRL revocation code, where this is linked to a certificate serial number and does not appear in conjunction with the Certificate Holder’s name or other publicly identifiable information.

## Responsibility to protect private information

Cogito Group and the Lead Agency (on behalf of New Zealand Government) must ensure that the private information of Certificate Holders held by New Zealand Government PKI entities is physically and technically protected from unauthorised viewing, modification or deletion; in accordance with the requirements of the Privacy Act; and NZISM and PSR.

## Notice and consent to use private information

This is governed by the requirements of the Privacy Act and the New Zealand Government PKI Framework Privacy Plan as detailed in 7.2 above.

## Disclosure pursuant to judicial or administrative process

Private personal information of Certificate Holders will only be disclosed if required by law. Any request for such disclosure must be signed by the requestor and delivered in writing to the Lead Agency; who will authorise Cogito Group to disclose only the requested information. Subsequent disclosure will only occur if the request is authorised, lawful and in compliance will all relevant legislative and applicable organisational controls.

# 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.

# Applicable Law

The law of New Zealand shall govern the interpretation and enforcement of this PDS, the Subscriber Agreement, the CPS, and any other associated agreements.

The governance for this CPS and any relevant CP is by, are 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.

Cogito Group and the Lead Agency will operate the New Zealand Government PKI Framework so as to at all times comply with the:

1. Privacy Act 1993,
2. Official Information Act 1982,
3. Protected Disclosures Act 2000,
4. Evidence Act 1908, and
5. Protective Security Requirements (PSR), including the New Zealand Information Security Manual (NZISM).

# Dispute Resolution

If a dispute arises between the New Zealand Government and any participating party [Dispute], written notice must be provided so that the parties can meet to negotiate in good faith to resolve the Dispute [Dispute Notice]. Should the Dispute remain 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 must 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, with such proceedings to be conducted in accordance with the *Public Service Code of Conduct* and the *Employment Relations Act 2000*.

# Audit

All infrastructure elements in the New Zealand Government PKI, including the AoG Root CA, require auditing on a regular basis to ensure that they comply with the CPS and respective CP’s. The process of such audits is not publicly disclosed, other than as described in the CPS. The audit reports and other [C&A] Certification artefacts (including any Risk Assessments) will be made available to Subscribing Agencies in order that they can accredit the PKI Services as meeting their enterprise security requirements.

In addition to the CPS requirements, the NZISM security Certification and Accreditation policy requires the conduct of regular audits to ensure compliance with Lead Agency policies and criteria. The New Zealand Government PKI Framework complies with the NZISM defined periods and events that require audit reviews.

The Lead Agency gives further consideration to the results of such audits before possibly implementing any recommendations and will update the Risk Assessment accordingly Cogito Group will review and update the Security and Risk Management Plan (SRMP) based on the Lead Agency audit activities.

Cogito Group is expected to conduct internal audits at regular intervals of its PKI services delivered on behalf of the New Zealand Government, and to maintain international accreditation of these services, which requires annual independent audits against appropriate standards and schemes (such as WebTrust[[7]](#footnote-7) and ISO/IEC-21188:2006)[[8]](#footnote-8). The Lead Agency (on behalf of the New Zealand Government) reserves the right to conduct its own reviews of Cogito Groups audit [reports].

The Lead Agency will select independent, credible and recognised auditors from the New Zealand Government Security and Related Services (SRS) Panel.

## Frequency of Audit

See Section 13.

Each CA and RA requires an annual audit, more frequently where required by extra-ordinary events.

# Trust Marks

As a private PKI environment, the New Zealand Government PKI is not subject to any mandated external accreditation. However, it has been designed to reflect best practice and comply with the following standards:

1. Protective Security Requirements (PSR), see https://protectivesecurity.govt.nz/.
2. New Zealand Information Security Manual (NZISM), Version 2.4, dated November 2015, see http://www.gcsb.govt.nz/publications/the-nz-information-security-manual.
3. ISO/IEC-29115:2013, Entity authentication assurance framework (EAAF). Also available as ITU-T Recommendation X.1254.
4. ISO/IEC-CD-29003:, Evidence of Identity (EoI) Framework [Draft]
5. ISO/IEC-21188:2006, Public key infrastructure for financial services — Practices and policy framework.
6. ISO/IEC 15782-1:2009, Certificate management for financial services — Part 1: Public key certificates.
7. RFC 5280 – X-509 Certificate and Certificate Revocation List (CRL) Profile, see <https://tools.ietf.org/html/rfc5280>.
8. RFC 5652 – Cryptographic Message Syntax (CMS), see <https://tools.ietf.org/html/rfc5652>.
9. RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, see <https://tools.ietf.org/html/rfc3647>.
10. AICPA/CICA WebTrust Program for Certification Authorities, Version 1.0, August 2000.
11. AICPA/CPA WebTrust Service Principles and Criteria for Certification Authorities, Version 2.0, March 2011.
12. CPA Webtrust for Certification Authorities – SSL Baseline Requirements Audit Criteria, version 1.1, 31st January 2013.

1. In accordance with agency procedures; and ISO/IEC-CD-29003, Identity Proofing; or ITU-T Recommendation X.1254 (ISO/IEC 29115:2013), Entity Authentication Assurance Framework. [↑](#footnote-ref-1)
2. A *Certificate Holder Agreement* is also known as a *Subscriber Agreement* in PKI terms, though ‘Susbcriber Agreement’ in TaaS contract terms carries a different definition.. [↑](#footnote-ref-2)
3. Such as use of their private signing key being the equivalent of their written signature. [↑](#footnote-ref-3)
4. Note that the RA must immediately notify the relevant Subscribers Authority in such circumstance, in accordance with the CA/RA Incident Management Plan [↑](#footnote-ref-4)
5. ID-MAC is a ‘medium assurance’ entity, which equates to ‘Level of Assurance’ 2 – LoA2. Refer to the NZ Govt PKIF Core Obligations Policy for definitions of LoA and LoIP. [↑](#footnote-ref-5)
6. In accordance with the process detailed in the Incident Management Plan; as well as the Disaster Recovery and Business Continuity Plan (DRBCP) [↑](#footnote-ref-6)
7. Webtrust for Certification Authorities – SSL Baseline Requirements Audit Criteria, version 1.1, January 2013. [↑](#footnote-ref-7)
8. To the extent and level where such independent audit capability is available in New Zealand [↑](#footnote-ref-8)