## New Zealand Government Public Key Infrastructure Framework

### Status: DRAFT for review

### Introduction

The New Zealand Government Public Key Infrastructure Framework (PKIF) governs the use of digital certificates and cryptographic keys issued through the New Zealand Government Public Key Infrastructure (PKI) to assure the identity and protect the information of affiliated entities. These entities may include persons, devices, software applications and organisations acting for or on behalf of the New Zealand (NZ) Government.

The Framework describes the structure of the NZ Government PKI and the requirements for organisations to implement an accredited authority service able to issue digital certificates and cryptographic keys for use within the NZ Government closed community (the community of NZ government affiliated organisations). The framework does not support digital certificates and cryptographic keys for use outside of this community (e.g. publically accessible agency websites).

The design, implementation and operation of a PKI is important, as these represent attractive targets for attackers. If a PKI can be coerced into registering devices that ought not to be, or disclosing private information (such as signing keys) then an attacker can compromise the security of the network.

An x509-based PKI will require a number of physical and logical components, including a Certificate Authority (CA), a Registration Authority (RA), a root of trust, and a means of revoking certificates. The organisation operating this PKI will also need to establish processes and procedures around these physical and logical components.

For the majority of scenarios where a PKI is required to support the identification of end entity cryptographic devices, the use of the PKI will be restricted to within a single relying organisation. In such circumstances, the organisation needs to ensure that the processes and technology used are appropriately secured by following these key points:

•Implement an 'offline root' model, in which the root of the PKI is kept permanently disconnected from the network, and powered off, until it is required.

•Establish well-defined processes for enrolling and revoking devices into and out of the PKI. These should map to associated business activities to ensure that only those endpoints which are expected to form part of the trusted infrastructure actually have valid certificates, and that all activities associated with the PKI are authorised and audited.

The maximum Key lifetimes for both the ECC and RSA encryption algorithms for the New Zealand Government Root CA is 10 years (April 2026) and for Subordinate CA(s) is 5 years (April 2021), from the date of initial establishment (6th April 2016).

If multiple public sector organisations will rely on the certificates issued by a Certification Authority then a Certificate Policy (CP) and Certification Practice Statement (CPS) will need to be produced and made available to all parties. A CP describes the overarching policy for the PKI and the CPS describes the processes and practices that a CA follows to meet the CP when issuing certificates, and allows others to judge whether these processes and practices are appropriate to rely on. Organisations should use RFC3647 as a template for their CPS.

PKIs are attractive targets for attackers. The information they hold (specifically private keys) and the function they perform (provision of trust) mean that a failure of security within a PKI can have far-reaching and hard-to-detect consequences. For this reason, PKIs need to be well-protected against would-be attackers.

### New Zealand Government PKI Framework Objectives

The objective of the NZ Government PKIF is to enable:

* The rapid subscription and migration of New Zealand Government Agency devices from their legacy environments to the virtual common Government network (GNet);
* A common Government PKI trust point to support the delivery of better public services; and
* Agency PKI environments to migrate to a common service delivery model

The primary strategic objective is therefore to implement key management for multiple cryptographic methods to support different business processes on GNet and implement cost effective key management and a root trust point across the NZ Government community.

#### Risks

Phil – TBC: Summarise from the Lead Agency risk assessment.

Consequently:

•CESG strongly recommend that PKIs are not shared across communities who would have significantly different security expectations or operational considerations (such as sharing a PKI used for commercial entities with public sector organisations).

•The possible use of the PKI for non-IPsec services should be considered at the design stage. CESG recommend that separate sub CAs are used per technology function to prevent the malicious use of a compromised certificate across different services. Alternative approaches, such as the use of separate CPOID values, key usage, and extended key usage fields, could also be used.

•CESG do not recommend Pre-Shared Keys (PSKs), Group Domain of Interpretation (GDOI), and other approaches for establishing shared keys across end devices.

•All VPN devices should ensure the certificates they are relying on are valid. This should be achieved by ensuring they have access to, and use, mechanisms for checking the status of certificates within the PKI - such as Certificate Revocation Lists (CRLs) or via Online Certificate Status Protocol (OCSP).

•Devices should be configured to check the entire certificate chain for validity; the end entity certificate, any sub CA certificates, and the root certificate. CESG recommend that PKI hierarchies are no more than three layers deep.

#### Benefits

The overarching benefits identified from the provision of the NZ Government PKI include:

* Realising savings and efficiencies in resources and operational management effort of operating an Agency based PKI[[1]](#footnote-1).
* Improves NZ Government ability for information sharing.
* Reduces Public Sector operational risk.
* Improved coherency across Government ICT services.
* Assists in realising the Government ICT Strategy and Roadmap.
* Standardised PKI framework.

#### The Telecommunications as a Service (TaaS) programme has also identified various benefits associated with utilising GNet and the set of associated telecommunications services, including:

#### Allowing agencies to easily connect with each other and with their customers which in turn make it easier to securely deliver more citizen-centric, cross-agency services.

#### Suppliers recognise government as one customer which provides volume discounts and drives costs down.

#### The supplier panel represents the best services available which allows agencies to use the most up-to-date technology.

#### The services offered are fit-for-purpose and offered from a range of suppliers allowing agencies to choose which supplier and service best fits their business needs.

#### The ‘utility’ consumption model frees agencies up to focus their investment and energy on solutions for New Zealand citizens, rather than investing in technology.

#### Services are offered ‘as a service’ with no minimum term or volumes. Agencies only pay for what they use.

#### The services will be flexible to take advantage of innovative opportunities as they become available.

#### Being able to use a common trusted NZ Government PKI is fundamental to delivering these benefits through GNet.

#### Outcomes

In order to support the future delivery of NZ Government and wider public sector business services over the shared Government Network (GNet) there is a need to provide a level of assurance over who is accessing what. The most cost effective mechanism for providing this assurance is through a common Government public key infrastructure, underpinned by a central governance authority tasked with maintaining its integrity. The business services the PKI would look to support are:

**Web services** – In order to support secure web services presented to the GNet, trusted application security is required.

**Voice and video conferencing** – Providing secure voice and video transport (DTLS/SRTP) over the GNet needs to be supported by a root trust point and PKI.

**User Authentication** – PKI keys and certificates are one very secure method that can be used for user authentication, especially where high assurance and non-repudiation is required. Protocols such as SAML, OATH and others based on X.509 certificates can be used for Single Sign-On (SSO) over GNet and mutual authentication of both users and devices.

**Communities of Interest (CoI)** – Setting up CoIs is currently very difficult and time consuming. With a PKI in place in which every end-point is registered, it is possible to create CoIs by adding those endpoints to a group using a shared key, which means CoIs can be created very quickly and cheaply on an ad-hoc basis. GNet is an example of a permanent, large scale, CoI.

The primary outcome is therefore to have implemented a New Zealand Government PKI service, providing a Root Authority trust point and assurance over certificate issuance and cryptographic key management processes.

Initially this is to meet the requirements of providing access to GNet, but expanding over the coming years to meet all of the above business requirements.

### New Zealand Government PKI Framework Governance

The Department of Internal Affairs in its role as Lead Agency of the Telecommunications as a Service (TaaS) Government ICT Common Capability (ICT-CC) is responsible for ensuring service providers conform to the obligations and standards set out in the NZ Government PKIF.

Recommendations for accreditation are made to the Department of Internal Affairs ICT Shared Services Security & Risk Steering Group (S&RSG). The S&RSG are responsible for decisions relating to the accreditation of service providers within the NZ Government PKIF.

### New Zealand Government PKI Structure

The NZ Government Public Key Infrastructure (PKI) operates at three tiers of authority:

* Root Authorities that anchor the chain of trust;
* Subordinate Authorities, including:
  + Policy Authorities that enforce the policies under which certificates are issued;
  + Interoperability Authorities that provide de-militarized zone (DMZ) services between different classes or jurisdictional certificate authorities;
* Issuing Authorities that issue end device or user certificates.

#### Certificate Authority (CA) Numbering Schema

A unique numbering schema for CA’s is to be implemented under the Framework, consisting of the unique name and serial number of the CA: [NZGovtCA<Serial>]. The serial number schema is as follows:

* {00x} Root CAs
  + {001} ECC Root CA
  + {002} RSA Root CA
* {10x} Policy CAs
  + {101} ECC GNet Policy CA
  + {102} RSA GNet Policy CA
* {20x}
  + {201}
  + {202}
* {30x} = Issuing CA’s
  + {301}
  + {302}

#### Root Authorities

The primary tier of the NZ Government PKI is the Root Authority layer. The Framework defines two (2) root authorities in the Root Authority layer.



The two root authorities are distinguished by the encryption standards they support. NZ Government PKIF Root Authorities are protected and engineered at the CONFIDENTIAL security classification level[[2]](#footnote-2).

NZ Government Agencies are asked to trust the certificates issued by the NZ Government Root Certificate Authorities.

The Root Authorities use name constraints on the certificates issued to Policy CAs to limit the scope of certificates issued under each policy.

#### Subordinate Authorities

The second tier of the NZ Government PKI consists of Subordinate Authorities, primarily operating as Policy Authorities. The NZ Government PKIF does not define the number of authorities that are able to be supported at this layer, however each must be chained to at least one of the two defined Root Authorities to participate within the NZ Government PKIF.



The NZ Government PKIF defines the accreditation process and criteria for a new Subordinate Authority to be granted permission to be chained to a NZ Government PKI Root Authority.

Government PKIF Policy Authorities are protected, engineered and operated at no higher than the RESTRICTED security classification level.

#### ****Issuing Authorities****

The third tier of the NZ Government Public Key Infrastructure is the Issuing Authority layer. The NZ Government PKIF also does not define the number of authorities that are able to be supported at this layer, however each must be chained to at least one Policy Authority to participate within the NZ Government PKIF.



The NZ Government PKIF defines the accreditation process and criteria for a new Issuing Authority to be granted permission to be chained to a NZ Government PKI Root Authority.

Government PKIF Issuing Authorities are protected, engineered and operated at no higher than the RESTRICTED security classification level.

## PKI Artefacts Publishing and Distribution Points

Web Publishing Points

6. The following web publishing points are to be used for the Framework:

|  |  |  |
| --- | --- | --- |
| **Publishing Point** | **IP Addresses** | **Use Cases (Examples)** |
| http://cert.pki.govt.nz | 122.56.33.130, 122.56.53.66 | HTTP AIAs, Certificates: (<http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.crt>) (and same URI for .p7c files) |
| https://www.pki.govt.nz | 122.56.33.130, 122.56.53.66 | Policy website: (https://www.pki.govt.nz/policy/<policyname>.pdf) |
| http://crl.pki.govt.nz | 122.56.33.130, 122.56.53.66 | HTTP CDPs: (http://crl.pki.govt.nz/crl/NZGovtCA<serial>.crl) |
| http://ocsp.pki.govt.nz | 122.56.33.130, 122.56.53.66 | OCSP: (http://ocsp.pki.govt.nz/) |
| http://dir.pki.govt.nz | 122.56.33.130, 122.56.53.66 | LDAP CDPs: (ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList) |

## Evidence of Identity (EoI) Policy

The PKI Framework Evidence of Identity (EoI) policy is based on ISO/IEC-xxx Draft Standard. The EoI policy includes the model for proving levels of identity, summarised in the following section.

### Levels of Identity Proofing (LoIP)

This section details the identity assurance requirements for the PKI Framework, especially those in PKI operational and management roles, such as Operations Manager and RAOs. Each level defines characteristics and minimum criteria that MUST be met in order to gain and maintain accreditation at a particular level.

**LoIP 1 – Low Confidence**

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

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

**LoIP 2 – Moderate Confidence**

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

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

**LoIP 3 – High Confidence**

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

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

| Requirement | LoIP 1 | LoIP 2 | LoIP 3 |
| --- | --- | --- | --- |
| **Identity Verification** | | | |
| **Objective 1**: Identity is unique | Records within the context shall be checked for a duplicate entry. | | |
| **Objective 2**: Identity exists | Not checked | Proofing party shall get evidence that the identifying attributes exist in corroborative source(s) | Proofing party shall get evidence that the identifying attributes exist in authoritative source(s) |
| **Objective 3**: Identity is bound to a person | Not checked | The proofing party shall check binding to the identity using one of the following factors:  Something known by the subject that is not public information or reasonably accessible on the evidence of identity;  **or**  Something the subject is. | The proofing party shall check binding to the identity using two or more of the following factors:  Something known by the subject that is not public information or reasonably accessible on the evidence of identity;  **and/or**  Something possessed by the subject;  **and/or**  Something the subject is. |
| **Objective 4**: Identity’s status | Not checked  *No validated Security Clearance held.* | Proofing information should be verified against an authoritative source recording death.  *Validated RESTRICTED / CONFIDENTIAL Security Clearance held.* | Proofing information should be verified against an authoritative source recording death.  *Validated CONFIDENTIAL / SECRET / TOP SECRET Security Clearance held.* |

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

## New Zealand Government PKI Accreditation

Accreditation decisions relating to the NZ Government PKIF are made by the ICT Shared Services Security & Risk Steering Group from the Department of Internal Affairs in its role as Lead Agency of the Telecommunications as a Service Government ICT Common Capability.

### New Zealand Government PKI Accreditation Process

The NZ Government PKIF Accreditation process is a specific case of the ICT Shared Capabilities Security Certification Process (ICT-SCSCP)[[3]](#footnote-3) and includes compliance requirements for NZ Government PKI specific policies and artefacts as described in this framework.

### New Zealand Government PKI Approved Documentation Requirements

Ongoing compliance with NZ Government PKIF Policies, Criteria and Approved Documents is mandatory for Service Providers to achieve and maintain NZ Government PKIF Accreditation. The NZ Government PKIF Approved Documents are listed in the following table, which indicates compliance obligations[[4]](#footnote-4) and to whom they apply[[5]](#footnote-5).

| Requirement | CA | RA | Section |
| --- | --- | --- | --- |
| **New Zealand Government PKI Specific Policies** | | | |
| New Zealand Government PKI Framework Overview | O | O |  |
| New Zealand Government PKI Core Obligations Policy | X | X |  |
| New Zealand Government PKI Mandatory Security Requirements | X | X |  |
| New Zealand Government PKI Lead Agency Risk Assessment | X | X |  |
| Identity Proofing or Evidence of Identity (EoI) Policy | O | X |  |
| **New Zealand Government PKI Criteria** | | | |
| Privacy Impact Assessment (PIA) | X | X |  |
| ICT Shared Services Security Certificate (ICT-S3C) | X | X |  |
| **New Zealand Government PKI Specific Approved Documents (CA, RA)** | | | |
| CA Key Generation Ceremony Plan (and signatory record) | X |  |  |
| Cryptographic Key Management Plan (CKMP) | X | X |  |
| Certification Practice Statement (CPS) | X |  |  |
| Certificate Policy (CP) | X |  |  |
| Authority/Certificate Revocation List (ARL/CRL) Management Plan | X |  |  |
| Solution Architecture | X |  |  |
| **ICT Shared Services Security Certification Process – Approved Evidential Documents (CA, RA)** | | | |
| Service Provider Risk Assessment (SPRA) | X | X |  |
| Statement of Applicability (SoA) or Controls Validation Plan (CVP) | X | X |  |
| Security Risk Management Plan (SRMP) | X | X |  |
| System Security Plan (SSP) | X | X |  |
| Operations Manual (SOP) | X | X |  |
| Site Security Plan (SiteSP) | X | X |  |
| Personnel Security Plan (PSP) | X | X |  |
| Vulnerability Management Plan (VMP) | X | X |  |
| Incident Response Plan (IRP) | X | X |  |
| Business Continuity and Disaster Recovery Plan (DRBCP) | X | X |  |
| Change Management Plan (CMP) | X | X |  |
| Security Risk Remediation Plan (SRRP) | X | X |  |
| Security Assurance Roadmap (SAR) | X | X |  |

### New Zealand Government PKI Accreditation Criteria

#### ICT Shared Services Security Certification Approved Artefacts

The detailed input and output description for the ICT Shared Services Security Certification artefacts is described in [ICT-SCSCPG].

#### New Zealand Government PKI Specific Approved Documents

The Certificate Authority (CA) is the core component of a PKI which issues digital certificates. The digital certificates bind a Subscriber’s identity (i.e. subject name) to the public key in the certificate. The CA is also responsible for digital certificate lifecycle operations, including the revocation of certificates. This is generally achieved through the use of CRLs, OCSP, or a combination of both.

In order to implement a CA effectively, a series of policies are used to govern its operations, including the CKMP, CRL Management Plan, CPS and CP.

* The CPS is a public document which describes the practices that the CA service will employ in managing the certificates it issues. These statements describe the PKI certificate framework, mechanism supporting the application, issuance, acceptance, usage, suspension/revocation and expiration of certificates signed by the CA, and the CA’s legal obligations, limitations and miscellaneous provisions. This document is evaluated against [PRA2005], [Priv2013], [RFC3647] and for compliance with the NZ Government PKIF Core Obligations Policy.
* The CP is a document which defines a named set of rules regarding the applicability of a certificate to a particular community and/or class of applications with common security requirements. A CP may be used by a Relying Party to help in deciding whether a certificate and the binding therein are sufficiently trustworthy and otherwise appropriate for a particular application. Similar to the CPS, this document is evaluated against [PRA2005], [Priv2013], [RFC3647] and for compliance with the NZ Government PKIF Core Obligations Policy.
* The CKMP identifies the implementation, standards, procedures and methods for key management in the related CA. The security of information protected by PKI directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with the keys and the protection afforded the keys. All keys need to be protected against modification, and private keys need to be protected against unauthorised disclosure. Key management provides the foundation for the secure generation, storage, distribution, use and destruction of keys. This document is evaluated as describing an appropriate CKMP for the related CA against the topics identified in the NIST Framework for Designing Cryptographic Key Management Systems [NIST SP800-130] and the NIST Recommendation for Key Management: General [NIST SP800-57Pt1.Rev4].
* The CRL Management Plan identifies the method and mechanism for creation and publication of the CA Certificate Revocation List. When a certificate is issued, it is expected to be in use for its entire validity period, however, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. In such circumstances, systems relying on the certificates must be able to ensure the certificate is still valid. The CRL Management Plan is evaluated against the requirements set out in RFC5280.
* The Solution Architecture describes the overall architecture of the specific system implemented by the CA. It should encompass the entire environment used to deliver the services of the CA. The solution architecture is not directly assessed, apart from for ensuring it accurately describes a complete solution, however it provides the key context for the assessment of the remainder of the artefacts.

Other documents SHOULD also be used, such as service contracts (and associated terms and conditions) or a Subscriber Agreement, which defines the undertakings that Subscriber’s will make in order to obtain and use certificates confirming their identity. It is expected that this will be part of the terms and conditions used to encourage user participation in digital service delivery. It is also expected that the Subscriber Agreement will include references to Relying Parties and their responsibilities, or references to Relying Party Agreements, which may also require evaluation.

**Shared PKI services**

There are situations where it is useful for multiple organisations to use a single shared PKI service, which may extend beyond the provision of certificates for IPsec devices. This service might be operated by one of the organisations on behalf of a wider community, or be provided by a commercial supplier for the purpose of supporting a community of VPN links.

In addition to the requirements above regarding the Certification Practice Statement, the following points relating to the central PKI infrastructure should be implemented by the PKI provider if their PKI is to be shared across multiple organisations.

**1. Data-in-transit protection**

Application-layer protection should be used to protect the integrity and authenticate requests and responses from the PKI service. Private keys should never be exchanged over such links, and certificates should always be authenticated, either using established points of trust, or via out-of-band mechanisms. For more information see [Cloud Security Principles](https://www.cesg.gov.uk/guidance/cloud-security-guidance-summary-cloud-security-principles).

**2. Asset protection and resilience**

Users of the PKI service should have confidence that their data, and the assets storing or processing it, will be protected against physical tampering, loss, damage or seizure

In practice, this means:

* Organisations using the PKI should be provided with information on where their data will be stored, processed and managed from.
* The physical security of locations providing the PKI service should be independently validated via CSA CCM v3.0, ISO/IEC 27001 or SSAE-16 / ISAE 3402.
* The PKI service provider's procedures for physical security of media should be independently validated via CSA CCM v3.0, ISO/IEC 27001 or SSAE-16 / ISAE 3402.
* Components within the service provider's architecture performing security-enforcing functions should be validated to Foundation Grade where available.
* Assured products should be used to perform sanitisation of media containing user information before disposal. Products should have Foundation Grade certification against the relevant [Data Sanitisation Security Characteristic](https://www.cesg.gov.uk/security-characteristics-collection). Alternatively, a certified destruction service, such as those certified under the [CESG Assured Service (Destruction) scheme](https://www.cesg.gov.uk/documents/cesg-assured-service-cas-service-requirement-sanitisation) .

**3. Separation between customers of the PKI service**

Logical separation between different customers of the PKI should be designed and implemented to prevent a single malicious or compromised customer of the PKI service from affecting the service or data of another.

Network and logical access to the PKI service should be restricted to only those organisations and individuals with a business requirement to use it.

A CCP-certified 'IA Architect' at the Senior or Lead level should be involved in the design or review of the PKI service architecture. This will ensure that the architecture defends against common attacks, has appropriate security controls, and allows effective secure operation of the PKI service.

**4. Governance framework**

The PKI service provider should have a security governance framework that coordinates and directs their overall approach to the management of the PKI and information within it.

In practice, this means:

There must be a clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the PKI service. This is typically someone with the title of Chief Security Officer, Chief Information Officer or Chief Technical Officer.

A documented framework must exist for security governance, with policies governing key aspects of information security relating to the PKI.

Security and information security should form part of the service provider’s financial and operational risk reporting mechanisms.

Processes exist to identify and ensure compliance with applicable legal and regulatory requirements relating to the PKI.

**5. Operational security**

The PKI service provider should have processes and procedures in place to ensure the operational security of the PKI. The PKI will need to be operated and managed securely in order to impede, detect or prevent attacks against it.

In practice, this means:

* The status, location and configuration of service components (including hardware and software components) are tracked throughout their lifetime within the PKI.
* Changes to the PKI are assessed for potential security impact. Changes are managed and tracked through to completion.
* Relevant sources of information relating to threat, vulnerability and exploitation technique information are monitored by the PKI provider.
* Known vulnerabilities within the PKI are tracked until sufficient mitigations have been deployed through a suitable change management process.
* 'Critical' patches should be deployed within 14 calendar days of a patch becoming available; 'important' patches should be deployed within 30 calendar days.
* Events generated in PKI components required to support effective identification of suspicious activity are collected and fed into an analysis system.
* Incident management processes are in place for the PKI and are enacted in response to security incidents. These should be validated using one of ISO/IEC 27035:2011, CSA CCM v3.0, or ISO/IEC 27001.

**6. Supply chain security**

PKI service providers often rely on third-party products and services. Those third parties can have an impact on the overall security of the PKI service. The service provider should ensure that any third parties that it relies on to securely provide its PKI service (such as a hosting service) also meet relevant security principles from this document to an appropriate level.

**7. Identity and authentication**

Consumer and service provider access to all PKI interfaces should be constrained to authenticated and authorised individuals. Weak authentication or access control may allow unauthorised changes to the PKI, leading to theft or modification of data, or denial of service.

It is also important that authentication occurs over secure channels. Use of insecure channels such as email, HTTP or telephone can be more vulnerable to interception or social engineering attacks.

**8. External interface protection**

All external or less trusted interfaces of the PKI service should be identified and have appropriate protections to defend against attacks through them.

If an interface is exposed to PKI consumers or outsiders and it is not sufficiently robust, then it could be subverted by attackers in order to gain access to the PKI or data within it. If the interfaces exposed include private interfaces (such as management interfaces) then the impact may be more significant.

**9. Audit and monitoring**

The PKI service provider should ensure that all activities which:

* cause the set of certificates issued by the CA to change (eg addition, deletion, alteration), or
* otherwise affect the secure operation of the PKI

shall be audited in such a manner as to ensure traceability of action, identified individual, and, where applicable, business process.

Access to the audit log shall be read-only by appropriately authorised individuals. Auditing mechanisms shall be designed to protect the integrity of the audit information after creation so that a failure or compromise does not directly compromise previous audit information.

**PKI Assurance**

Beyond the requirements outlined above, there is no requirement for extra independent assurance in the PKI service offering. Providers offering PKI services to multiple customers may wish to independently demonstrate that, in practice, their processes achieve the principles outlined in their Certificate Policy and have been implemented as described in their Certificate Practice Statement, through use of approaches such as [T scheme](http://www.tscheme.org/).

## References

|  |  |
| --- | --- |
| Reference | Description |
| [ICT-SCSCPG] | The Department of Internal Affairs’ ICT Shared Capabilities Security Certification Process Guidance |
| [NIST SP800-130] | NIST Special Publication 800-130: Framework for Designing Cryptographic Key Management Systems |
| [NIST SP800-57Pt1.Rev4] | NIST Special Publication 800-57, Part 1 Revision 4: Recommendation for Key Management |
| [PRA2005] | New Zealand Public Records Act 2005 |
| [Priv2013] | New Zealand Privacy Act 1993; incorporating the Privacy Amendment Act 2011 and Privacy Amendment Act 2013 |
| [RFC3647] | IETF Request for Comments 3647: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework |
| [RFC5280] | IETF Request for Comments 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |

## Attribution

This document is based on extracts from:

Gatekeeper PKI Framework: © Commonwealth of Australia 2015.

*PKI Implementation Strategy version 1.0 (28/02/13)*: Public Services Network Programme, UK Government

1. The cost savings per agency or system instance (ie. Some agencies operate multiple PKI instances/systems) are in the region of $30k OPEX each per year, and $300-600k each per year CAPEX. [↑](#footnote-ref-1)
2. In accordance with the Information Security Management Protocol from the PSR [↑](#footnote-ref-2)
3. Guidance to the ICT-SCSCP is provided in [ICT-SCSCPG]. [↑](#footnote-ref-3)
4. Key for the table: “X” is mandatory/required; “O” is optional. [↑](#footnote-ref-4)
5. Service Providers may provide combined documentation, where this is appropriate and assists security audit review purposes. [↑](#footnote-ref-5)