nbn Public Key Infrastructure - Certificate Policy

Document Owner	**nbn** PKIPA
Status	Final
Issue date	29 OCT. 25
Revision number	2.4

Document control

Document Management

This document is controlled by:	**nbn** co Public Key Infrastructure Policy Authority (PKIPA)

Revision history

Date	Revision	Details
25 Nov. 11	1.0	Initial release version.
17 Nov. 20	2.0	Released with revisions.
3 Nov. 22	2.2	Updated details of issuance types.
24 Nov. 23	2.3	Minor updates.
29 Oct. 25	2.4	Updates for migration to new platform.

Contents

1. Introduction

Certificate policies are, in the X.509 version 3 digital certificate standard, the named set of rules regarding the applicability of a certificate to a particular community and/or class of applications with common security requirements. A Relying Party may use a CP to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application.

This Certificate Policy (CP) identifies the rules to manage the **nbn** Root Certificate Authority (CA) certificates, Subordinate-Certificate Authority (Sub-CA) certificates and associated core component certificates. It includes 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 **nbn** PKI Certification Practice Statement (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 CP follow the framework set out in the Internet Engineering Task Force 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 this CP. The provisions of this CP prevail over the provisions of CPS to the extent of any direct inconsistency. The provisions of CPS govern any matter on which this CP is silent. (Note: where subtitled sections of the framework provide no additional information to detail provided in the CPS they have not been further extrapolated in this document.)

1. NBN Co has a PKI Framework that consists of a set of specifications and requirements governing the implementation and operation of Certification Authorities, Registration Authorities, and other PKI components; and deals with:
    a. PKI Technical Standards,
    b. Certificate Policies (CP), including this CP,
    c. Requirements for Certification Practice Statements (CPS), and
    d. Any Subscriber or Relying Party Agreements, templates and other NBN Co PKI guidelines.
2. This Certificate Policy (CP) only applies to any certificates issued by, or under the authority of, NBN Co Limited or any of its entities directly or subsequently under the NBN Co Limited Root Certification Authority (NBN Co Root CA) within the NBN Co Public-Key Infrastructure (NBN Co PKI).
3. Expressions used in this CP are defined in the glossary in Appendix A which can be found at the NBN Co website and https://pki.nbnco.net.au/.
4. This Certificate Policy and any corresponding Certification Practising Statements are policy documents and do not form (and are not intended to form) legally binding agreements. Contractual obligations will be set out in other agreements such as Subscriber Agreements and Relying Party Agreements.

1.1 Overview

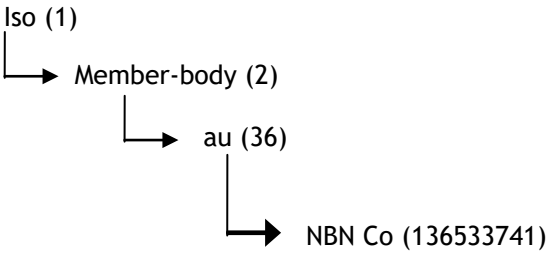
1. The NBN Co PKI is an IETF1 “Public-Key Infrastructure (X.509)” (PKIX) implementation of an ITUT X.509 PKI, supporting various levels of authentication assurance and confidentiality for electronic communications between the distributed information systems of the NBN Co and its clients, suppliers, partners, and employees.

1.2 Document Name and Identification

1. Document Name: **nbn Public Key Infrastructure - Certificate Policy**
2. Document Public Location: https://pki.nbnco.net.au/CP

1.2.1 Policy Object Identification

1. Each level of certification assurance has an assigned object identifier (OID) to be asserted in the Certificate Policies extension of certificates issued by CAs who comply with the applicable policy requirements.
2. The NBN Co Limited registered OIDs are as follows:



This CP defines multiple certification Assurance Levels that are subordinate to the NBN Co arc as follows;

1.2.36.136533741.1	NBNCo Public Key Infrastructure – Certificate Practices Statement
1.2.36.136533741.2	NBNCo Assurance Level arc
1.2.36.136533741.2.1	Not in current use
1.2.36.136533741.2.2	NBNCo Standard Private Certificate Issuance
1.2.36.136533741.2.3	NBNCo High Assurance Level
1.2.36.136533741.3	NBNCo Medium Assurance Level G3
1.2.36.136533741.3	NBNCo Medium Assurance Root CA G3
1.2.36.136533741.3.1	NBNCo Basic Assurance Corporate Issuing CA G3
1.2.36.136533741.3.2	NBNCo Basic Assurance NTF Issuing CA G3
1.2.36.136533741.3.3.1	NBNCo Basic Assurance Active Networks Issuing CA1 G3
1.2.36.136533741.3.3.2	NBNCo Basic Assurance Active Networks Issuing CA2 G3

1.2.2 Related documents

Table 1 – Related documents

Document	Owner	Availability
[1] **nbn** Public Key Infrastructure – Certificate Practice Statement	nbn	Public
[2] **NBN** Co Public Key Infrastructure Framework Overview	nbn	Internal
[3] Master Services Agreement	DigiCert	Public
[4] Relying Party Agreement	DigiCert	Public

Document		Owner	Availability
[5]	Relying Party Agreement – User Certificates	DigiCert	Public
[6]	Registration Authority Practices Statement	DigiCert	Public

1.3 PKI Participants

1.3.1 Certification Authority Owner

1. The Certification Authority Owner (CAO) is the legal entity responsible for the Certification Authority.
2. For this CP, the CAO is NBN Co Limited.
3. Unless the context requires otherwise, any reference within this CP, and any associated CPS, Subscriber Agreement, and Relying Party Agreement, to the CAO, in relation to rights, obligations, acts, or omissions, shall include the entities to which the CAO has delegated a Trusted Role in accordance with Section 5.2.1

1.3.2 Policy Authority

1. The Policy Authority (PA) is the entity responsible for the approval of Certificate Policies, Certification Practice Statements, Subscriber Agreements, and Relying Party Agreements.
2. The PA for NBN Co PKI components is the NBN Co Public Key Infrastructure Policy Authority (NBN Co PKIPA).
3. From time-to-time the NBN Co PKIPA may appoint a PA Technical Advisory Group to assist it in meeting its obligations and responsibilities.

1.3.3 Certification Authorities

1. The Certification Authority (CA) that issues end-entity certificates under this CP is the NBN Co Root CA and its Subordinate CAs operated by NBN Co Limited. The functions and obligations of each Subordinate CA are the same as those of the NBN Co Root CA under this CP and the CPS.
2. This CP only applies to the end-entity certificates issued under the NBN Co Subordinate CAs.

1.3.4 Registration Authorities

1. The NBN Co Registration Authority (RA) or an NBN Co accredited RA will perform the functions of the Registration Authority.
2. Where an RA function under this CP is performed by a person other than the NBN Co RA, that RA will be bound by NBN Co to perform the Registration functions in accordance with the CP and other Approved Documents.

1.3.5 Subscribers

1. A Subscriber is an entity, whether an individual or organisation, to whom Certificates are issued.
2. Each Subscriber under this CP shall agree to be bound by the terms of the associated Subscriber Agreement in accordance with Section 4.4
3. Where a Subscriber delegates responsibility for initiating applications for Certificates to an automated system, the Subscriber shall ensure that the automated system meets the terms and conditions of the CP and the Subscriber Agreement.

1.3.6 Relying Parties

1. A Relying Party is an entity, whether an individual or organisation, which:
    a. Relies on the Binding of the Public Key to the Distinguished Name (DN) of a Subject in a Certificate to the level of certification assurance stated within that Certificate; or
    b. Distributes the Certificate of the CA as part of a PKI-aware application, or through any other means; or
    c. Distributes a PKI-aware application that accepts the Relying Party Agreement on behalf of an end user of that application or bypasses the requirement for such acceptance via some other mechanism.
2. Each Relying Party under this CP shall agree to be bound by the terms of the associated Relying Party Agreement in accordance with Section 4.4
3. Where a Relying Party delegates responsibility for validating Certificates to an automated system, the Relying Party shall ensure that the automated system meets the terms and conditions of this CP and the Relying Party Agreement.

1.3.7 Other Participants

1.3.7.1 Auditors and Assessors

1. The Auditor and Assessor roles used by the CA shall be detailed in the CPS and other NBN Co Approved Documents.

1.4 Certificate Usage

1. This CP supports three levels of assurance:
    - Basic
    - Standard/Medium
    - High
2. Basic Assurance:
    a. Basic assurance is suitable for certificates issued to a Device, service or process required to secure NBN Co communications, for a short-term basis of not more than 30 days.
    b. Must not be used on any PKI CA/RA components.
    c. Current usage of Basic Assurance under OID 1.2.36.136533741.2.1 is no longer used as there is no current identified use case where Basic assurance is only required. From the date of publication of this CP, all certificates requested under the 1.2.36.136533741.2 OID must use Medium/Standard Assurance or higher henceforth.
    d. Usage of Basic Assurance under 1.2.36.136533741.3 OID will continue to be used under the specific use cases of the Certificate Authority.
    e. Usage of Basic Assurance is including the following, but not limited to:
        i. Temporary device access to the network using certificate authentication.
        ii. Transitory servers such as containers.
3. Medium Assurance:
    a. Verification of the requestor; confirmation of membership to a **nbn** team email address that controls the requested certificate common name.
    b. Medium Assurance is suitable for authentication certificates issued for access to the NBN Co network or for digital signing certificates where loss of confidentiality, integrity and availability

could be expected to have a serious adverse effect on organisational operations, organisation assets or individuals.

c. Usage of Medium Assurance includes, but is not limited to, the following:
    i. Client authentication when to connecting to VPN or Internal Networks.
    ii. Intra-Server communication.
    iii. Server Certificate signing.
    iv. All other certificate signing requirements; where no compliance or business identified high transactional value signing is required. If any of these are required, then the certificate must be signed under High Assurance level and stored in an HSM.

4. High Assurance:
    a. High Assurance is suitable for authentication certificates issued for access to the NBN Co network or for digital signing certificates where loss of confidentiality, integrity and availability could be expected to have a severe or catastrophic adverse effect on organisational operations, organisation assets or individuals.
    b. Usage of High Assurance includes the following:
        i. Specific compliance requirement that the certificate be signed to a High Assurance level for example a PCI DSS compliance requirement; or
        ii. **NBN** Co has identified that the certificate is to be used on a service to be of high transactional value.
    c. The private key must be set to be non-exportable and hosted securely on a Hardware Security Module (HSM) device.

1.4.1 Appropriate Certificate Uses

1. Relying Parties shall undertake due diligence to ensure that the level of certification assurance provided in an NBN Co PKI certificate is suitable for their application. Such a Relying Party may then rely on any assertion of assurance provided by the certificate only within that level and shall then determine the resultant authentication in accordance with the NBN Co PKI Framework.
2. Where a Relying Party is satisfied that the level of certification assurance provided in a NBN Co PKI certificate is suitable for their application, such a Relying Party may use the certificate and the Public Key contained therein, for any purpose permitted by the Key Usage extension of the certificate and the NBN Co PKI Framework.

1.4.2 Prohibited Certificate Uses

1. No party shall use a Certificate issued under this CP for any assurance of any Key, value, attribute, property, or characteristic, for purposes or in a manner not permitted by the applicable Subscriber Agreement or Relying Party Agreement, the key Usage extension of the Certificate, and this CP.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

1. The NBN Co PKIPA is responsible for all aspects this CP.

1.5.2 Contact Person

1. The contact details for the NBN Co PKI Policy Authority are:

Email: pkipa@nbnco.com.au

1.5.3 Person Determining CPS Suitability for the Policy

1. The NBN Co PKIPA is the approving authority for every Certification Practice Statement under this CP and associated Subscriber Agreements and Relying Party Agreements.

1.5.4 CPS Approval Procedures

1. Every CA issuing any certificates asserting any of the OIDs described in Section 1.2.1 of this policy must provide, and have approved, its CPS in complete accordance with this policy.
2. Every CA issuing any certificates asserting any of the OIDs described in Section 1.2.1 of this policy must comply with all the provisions of this CP and the approved CPS, as determined by an independent auditor, in accordance with Section 8 of this CP, before issuing any such certificates.

1.6 Definitions and Acronyms

1. All definitions and acronyms are listed in 9.11 Appendix A of this document.

2. Publication and Repository Responsibilities

2.1 Repositories

1. The authoritative repository for all NBN Co PKI related documentation shall be located at https://pki.nbnco.net.au/ and made available to all Subscribers and Relying Parties of these Certificates in accordance with the applicable Subscriber Agreements and Relying Party Agreements.
2. Certificate revocation lists will be hosted in a separate repository located under the URL http://crl.nbnco.net.au/ for CA based certificates and http://crl.one.au.digicert.com/ for end entity certificates.
3. Repositories shall deploy access controls to protect information in accordance with Section 2.4

2.2 Publication of Certificate Information

1. This CP and the associated CPS shall be available from https://pki.nbnco.net.au/.
2. Certification Authority revocation status shall be available from http://crl.nbnco.net.au/ for CA based certificates and http://crl.one.au.digicert.com/ for end entity certificates.

2.3 Time or Frequency of Publication

1. Any changes made to the CP or CPS shall be published to the Repository in accordance with the notification requirements in Section 9.8
2. Certificate Status shall be made available in accordance with Section 4.10

2.4 Access Controls on Repositories

1. Repositories shall employ appropriate mechanisms to support the availability and security of all published information to meet the requirements of applicable Subscriber Agreements and Relying Party Agreements.

2. Confidential Information shall be handled in accordance with Section 9.3

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

1. The Certificates shall use X.500 Distinguished Names (DNs), constructed from Relative Distinguished Names (RDNs) ordered from the hierarchy root to the leaf nodes.

3.1.2 Need for Names to be Meaningful

1. The Certificate DNs, including each of the RDNs, shall in all cases be meaningful. That is, each RDN shall be meaningful within the context of its parent component.
2. SAN (Subject Alternate Names) are supported, a maximum of 18 SANs are permitted in a single certificate.
3. Wildcard certificates cannot be used without the approval of the **nbn** PKIPA or its delegate.

3.1.3 Anonymity or Pseudonymity of Subscribers

1. Certificates shall not be issued for anonymous Subscribers under the NBN Co PKI.
2. All certificates except subscriber certificates must be assigned to mailing distribution list that is within the **nbn** email domain upon certificate enrolment.
3. CA certificates shall not be issued for anonymous or pseudonymous subscribers under the NBN Co PKI.
4. This does not include role-based certificates if the role is correctly identified.
5. This does not include certificates issued for an officially recorded identifier, such as a device identifier.

3.1.4 Rules for Interpreting Various Name Forms

1. DNs shall be interpreted according to the X.501 standard:
    a. Country [countryName] (C) – This attribute contains a two-letter ISO 3166 country code.
    b. Organisation [organizationName] (O) – This attribute contains the name of an organisation.
    c. Organisational Unit Name [organizationalUnitName] (OU) – This attribute contains the name of an organisational unit or department (optional field)
    d. Common Name [commonName] (CN) – This attribute contains a name of an object.

3.1.5 Uniqueness of Names

1. Each DN assigned to a Subscriber under this CP shall be unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

1. No Stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

1. Where the Subscriber does not generate the Private Key, this is not applicable.
2. Where the Subscriber does generate the Private Key, proof of possession shall be performed by provision of PKCS #10 Certificate Signing Request (CSR) or equivalent methods.
3. If the Subscriber does not generate the Private Key, then the delivery process by which the Private Key is transferred to the Subscriber must be auditable. Refer to Section 6.1 and 6.2

3.2.2 Authentication of Organisation Identity

1. The identity of a Subscriber that is an organisation shall be authenticated as follows:
    a. A RO shall:
        i. Verify the identity of the Subscriber; and
        ii. Verify any delegation of authority by the Subscriber.

3.2.3 Authentication of Individual Identity

1. The identity of a Subscriber that is an individual shall be authenticated as follows:
    a) A RO shall:
        i. Verify the identity of the Subscriber.

3.2.4 Non-verified Subscriber Information

1. Prior to certificate issuance all information required in a certificate must be verified to meet the requirements of the Assurance Level sought as defined in Section 1.4.1

3.2.5 Criteria for Interoperation

1. The NBN Co PKIPA may make decisions about interoperability with another PKI Subject to the policies defined in this CP and with the approval of NBN Co Limited.

3.3 Identification and Authentication for Re-key Requests

1. Prior to any NBN Co CA Certificate re-key activities, NBN Co will verify that the re-key activity has been requested by an authorised entity.

3.3.1 Identification and Authentication for Routine Re-Key

1. Policies relating to re-key requests are defined in Section 4.7
2. For Basic and Standard/Medium Assurance Certificate re-key requests the Subscriber's identity:
    a. may be established through use of the current signing key; and
    b. must meet the criteria defined in Section 1.4 at the time the re-keyed certificate becomes valid.
3. High Assurance certificates and any certificates shall not be re-keyed on the basis of a current valid certificate and the Initial Identity Validation shall be undertaken each time.
4. The certificate will also generate a new private key except for certificates used for S/MIME encryption purposes.

3.3.2 Identification and Authentication for Re-Key After Revocation

1. Re-key is not allowed after revocation for CAs.
2. Re-Key after revocation shall occur in the same manner as for initial identity validation.

3.4 Identification and Authentication for Revocation Requests

1. The parties who can make a request for the revocation of a certificate are identified in Section 4.9.2

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

1. All applicants must successfully complete the Initial Identity Validation in accordance with Section 3.2 of this CP.

4.1.1 Who Can Submit a Certificate Application

1. An application for a CA certificate must be submitted to the NBN Co PKIPA by the Certificate Authority Manager (CAM) of the applicant CA.
2. An application for a Registration Authority (RA) certificate must be submitted to the NBN Co PKIPA by one of the following:
    a. the CAM of the CA that will generate the certificate for the applicant RA.
    b. the higher-tier RA of the applicant RA.
3. An application for an individual Subscriber certificate must be submitted by one of the following:
    a. the Registration Officer for an RA with the approval of the Subscriber's Manager / Section head.
    b. the Subscriber's Manager / Section head.
    c. the Subscriber with the approval of their Manager / Section head.
4. An application for a Subscriber certificate for a Device or service shall be submitted by the custodian of the Device or service.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 CA Certificates

1. To enrol an Issuing Certification Authority in the NBN Co PKI hierarchy the following must occur:
    a. The CA applicant must complete and submit an application to the NBN Co PKIPA, supported by the documentation identified in the NBN Co PKI Framework document.
    b. NBN Co PKIPA must approve the enrolment of the CA in the NBN Co PKI before any certificates are issued.
2. Issuing CA certificates will have the Path Length Constraint within the Basic Constraints section of the certificate set to 0 thusly, no additional CA can be created a lower level.

3. All CA certificates must have the Key Usage Purposes set to ‘Certificate Signing’ and ‘CRL Signing’ only as per Section 6.1.6

4.1.2.2 RA Certificates

1. To enrol a Registration Authority in the NBN Co PKI the applicant must:
    a. be identified at a High Assurance Level as per the NBN Co PKI Framework,
    b. complete and submit an application to the NBN Co PKIPA.
2. The NBN Co PKIPA must:
    a. arrange an Accreditation Audit of the RA as part of the enrolment process,
    b. approve the enrolment of the RA in the NBN Co PKI before any certificates are requested by the RA.

4.1.2.3 End-User Certificate Subscribers

1. The process to obtain a certificate requires the completion of the following steps:
    a. The applicant or the applicant’s manager must complete and submit an application,
    b. The applicant must be identified by the CA or the delegated RA in accordance with the NBN Co PKI requirements for the Assurance Level for the requested certificate, and
    c. The applicant must provide information and evidence to confirm their identity; in accordance with the NBN Co PKI requirements for the Assurance Level for the requested certificate.

4.2 Certificate Application Processing

1. The CA will conduct the certification process in accordance with this CP and the CPS.

4.2.1 Performing Identification and Authentication Functions

1. The Identification and authentication of the Subscriber shall be performed by the CA or the delegated RA.

4.2.2 Approval or Rejection of Certificate Applications

1. The CA or the delegated RA must:
    a. Verify the authority of the applicant that submits a certificate application, and
    b. Verify the integrity of the information in the certificate request.
2. The CA or the delegated RA may reject a Certificate Application.
3. A Certificate Application shall not be considered accepted until the CA or the delegated RA has accepted the application and decided to issue a certificate.

4.2.3 Time to Process Certificate Applications

1. There is no time limit for the NBN Co PKIPA or its delegates to consider a Certificate Application.

4.3 Certificate Issuance

1. The CA will generate, sign, and publish the certificate and forward a copy of the certificate to the Subscriber.

4.3.1 CA Actions during Certificate Issuance

1. The CA must:
    a. Authenticate the request,
    b. Ensure uniqueness of the request,
    c. Obtain proof of possession of the Private Key,
    d. Assign a unique serial under the current CA key,
    e. Sign the certificate,
    f. Issue the certificate to the Subscriber, and
    g. Publish the certificate to the repository in accordance with Section 4.4.2

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

1. The Subscriber or the custodian of a Device or service shall be informed of the creation of a certificate and its availability.

4.4 Certificate Acceptance

1. Before the first subsequent use of the Private Key matching the Public Key in a certificate, the Subscriber shall agree to all Subscriber obligations and responsibilities in this CP and the CPS.

4.4.1 Conduct Constituting Certificate Acceptance

1. The first subsequent use of the Private Key matching the Public Key in the certificate shall function as both acknowledgement of receipt and acceptance of the certificate, unless the CA has chosen to require explicit formal acceptance to provide a higher level of assurance.

4.4.2 Publication of the Certificate by the CA

1. Certificates are published on creation. Should the requirements of Certificate Acceptance not be met, the certificate shall be revoked.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

1. The NBN Co PKIPA must be notified whenever any CA operating under this CP issues a CA certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

1. The Subscriber's Private Key must:
    a. Never leave the device on which it is stored. For NBN Co High Assurance certificates the associated Private Keys must be secured by hardware (Hardware Security Module).
    b. Not be used after the expiration unless renewed.
    c. Not be used after revocation of the certificate unless for the following revocation reasons:
        i. cACompromise - if the CA certificate private key was stolen or become known to an unauthorised entity,
        ii. cessationOfOperation - when a subscriber leaves the company, or device is decommissioned, or

iii. certificateHold – a temporary revocation of a certificate.

d. be used in accordance with the terms and conditions in this policy; and

e. only be used for NBN Co approved applications consistent with the certificate content.

2. No copy of any High Assurance or Medium Assurance Authentication/Signature Private Key shall be held by any entity other than the Subscriber.

4.5.2 Relying Party Public Key and Certificate Usage

1. A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.
2. Relying Parties ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension if the extension is present. If the extended key usage extension is present and implies any limitation on the use of the certificate, those constraints shall also be followed.
3. Relying Parties should assess:
    a. The restrictions on key and certificate usage are specified in critical certificate extensions, including the basic constraints and key usage extensions, and
    b. The status of the certificate and all the CA certificates in the certificate chain. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to determine whether reliance on a Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.
4. Validation should comply with Section 6 'Certificate Path Validation' of IETF RFC 5280 or use a validation authority that confirms with IETF RFC 3029.

4.6 Certificate Renewal

1. Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number.

4.6.1 Circumstance for Certificate Renewal

1. A certificate may be renewed if the certificate has not expired, the certificate has not been revoked, the certificate information is still correct, and the total lifetime of the Private Key has not been exceeded. The Subscriber must ensure that the private key's total lifetime from when it was first created and until the expiry of the renewed certificate that this will not exceed the maximum lifetime permitted under this CP for that key, as detailed in Section 6.3.2
2. Certificate renewal must be completed at least 30 days prior to the expiration of the certificate to ensure that adequate time is available to triage any issues with the certificate installation.
3. Upon certificate renewal, revocation of the previous certificate must also be completed as part of the same change to ensure that the certificate has correctly installed.

4.6.2 Who May Request Renewal

1. It is the sole responsibility of the Subscriber to ensure the prompt renewal of the certificate before the expiry date.

4.6.3 Processing Certificate Renewal Requests

1. Verification of Subscriber information for renewal requests shall be conducted in accordance with Section 3.2.4
2. High Assurance certificates and any certificates asserting to a High Assurance Level must not be renewed on the basis of a current valid certificate and the Initial Identity Validation shall be undertaken each time.

4.6.4 Notification of New Certificate Issuance to Subscriber

1. Refer to Section 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

1. Refer to Section 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

1. Refer to Section 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to other Entities

1. Refer to Section 4.4.3

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

1. A certificate may be re-keyed only if:
    a. the certificate to be re-keyed is valid at the time the re-key operation is conducted.
    b. the certificate is issued with either Basic or Medium level assurance.
    c. the Subject of the certificate meets the criteria in:
        i. Section 3.1.1
        ii. Section 3.1.2
        iii. Section 3.1.3
    d. The Distinguished Name (DN) in the certificate is to be identical in the new certificate.
2. The RA certifies that the Subscriber will meet the criteria defined in Section 1.3.4 at the time the re-keyed certificate becomes valid.
3. A new Public Key will be used in the new certificate to be issued. Specifically, an existing Public Key must not be used.
4. A re-key of a CA certificate may be considered if:
    a. the certificates that are to be issued by a CA will have an expiry date no later than the Issuing CA expiry date, or
    b. A CA updates its Private Key resulting in a new Public Key to be added to a certificate.

4.7.2 Who May Request Certification of a New Public Key

1. Subject to the requirements of Section 3.3 a re-key request can be made by:
    a. a Subscriber who is the Subject of the certificate,
    b. the Subscriber's officer-in-charge / section head,

c. the custodian of a Device or service,
d. an RA, or
e. a CA Manager.

2. All requests to re-key RA/CA certificates must be approved by the NBN Co PKIPA.

4.7.3 Processing Certificate Re-keying Requests

1. Verification of Subscriber information for re-key requests shall be conducted in accordance with Section 3.2.4
2. Identification and authentication for re-key requests shall be conducted in accordance with Section 3.3

4.7.4 Notification of New Certificate Issuance to Subscriber

1. Refer to Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

1. Refer to Section 4.4.1

4.7.6 Publication of the Re-keyed Certificate by the CA

1. Refer to Section 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to other Entities

1. Refer to Section 4.4.3

4.8 Certificate Modification

1. Once issued a Subscriber certificate cannot be modified under this CP.

4.8.1 Circumstance for Certificate Modification

1. Modifying a certificate means creating a new certificate for the same subject with information that differs slightly from the old certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with the CP and CPS. The new certificate may have the same or a different subject public key.
2. A CA operating under this policy may modify the information in a CA certificate if:
    a. the certificate to be modified is valid at the time the modification is conducted,
    b. the modified Certificate maintains the same level of trust and assurance as the original issued certificate,
    c. the subject name did not change, and
    d. the EKU of the certificate is not more restrictive than the previously issued.
3. The original certificate may be revoked, but cannot be further re-keyed, renewed, or modified.

4.8.2 Who May Request Certificate Modification

1. Subject to the requirements of Section 3.3 a certificate modification request can be made by:
    a. the CAM
    b. the NBN Co PKIPA

2. The NBN Co PKIPA must approve modification of a CA certificate.

4.8.3 Processing Certificate Modification Requests

1. The CAM or NBN Co PKIPA must verify all changes to certificate information before a modified CA certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

1. No Stipulation.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

1. Refer to Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

1. Refer to Section 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to other Entities

1. Refer to Section 4.4.3

4.9 Certificate Revocation and Suspension

1. CAs operating under this policy shall issue CRLs covering all unexpired certificates issued by the CA.
2. The CRLs shall conform to IETF PKIX, RFC 5280 as per section 7.2 of this CP.
3. Suspension of certificates is not allowed under this policy.

4.9.1 Circumstances for Revocation

1. A certificate shall be revoked when the binding between the Subscriber identified in the Subject Name field and the Public Key defined within the certificate is no longer considered valid.
    a. Examples of circumstances that invalidate the binding are:
        i. the certificate is modified as per Section 4.8
        ii. a change in any identifying information or affiliation components that necessitate a change in DN or SAN,
        iii. the Subscriber's keys or certificate are no longer required by the Subscriber, for example, on termination of employment,
        iv. privilege attributes asserted in the certificate are reduced,
        v. the certificate information is inaccurate, for whatever reason,
        vi. the Subscriber or CA identified in the Subject Name field can be shown to have violated the terms and conditions of this policy,
        vii. there is reason to believe the Private Key or media holding the Private Key has been compromised,
        viii. the Subscriber identified in the Subject Name field or other Authorised Party (as defined in the CPS) asks for his/her certificate to be revoked, or
        ix. the Device or service identified in the Subject Name field is decommissioned.

b. Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL.

2. A Certificate may be revoked at the direction of the NBN Co PKI PA.
3. The RO may make reasonable enquiries in accordance with arrangements agreed with the Subscriber to verify the accuracy of any reported Private Key compromise.

4.9.2 Who Can Request Revocation

4.9.2.1 CA Certificates

1. A request to revoke a CA Certificate must be made by one of the following:
   a. the CAM of the CA whose certificate is to be revoked, or
   b. the NBN Co PKIPA.

4.9.2.2 RA Certificates

1. A request to revoke a RA Certificate must be made by one of the following:
   a. the RAM of the RA whose certificate is to be revoked,
   b. the CAM of the CA that issued the certificate; or
   c. the NBN Co PKIPA.

4.9.2.3 Subscriber Certificates

1. A request to revoke a Subscriber certificate may be made by one of the following:
   a. the individual Subscriber identified in the Subject Name field of the certificate,
   b. the Officer-in-Charge / Section Head of the individual Subscriber identified in the Subject Name field of the certificate,
   c. the Manager, HR, or his/her delegate when the period of employment of a staff member or contractor with **nbn** is terminated,
   d. the custodian of a Device or service,
   e. a Registration Officer or RAM on behalf of the NBN Co PKIPA,
   f. the CAM of the CA that issued the certificate, or
   g. a member of the NBN Co PKIPA.

4.9.3 Procedure for Revocation Requests

1. Revocation requests are to be submitted to the CA and shall:
   a. identify the certificate to be revoked,
   b. explain the reason for revocation, and
   c. allow the request to be authenticated (e.g., digitally, or manually signed).
2. The CA will:
   a. review the current certificate status and no action will be taken if:
      i. the certificate has expired,
      ii. the certificate will expire within the CRL validity period, or
      iii. the certificate has already been revoked.
   b. authenticate requests,
   c. add the Revoked Certificates to the CRL, and
   d. publish the CRL in accordance with Section 2.2
3. Revoked certificates shall be included on all new publications of the Certificate Revocation List until the certificates expire.

4.9.4 Revocation Request Grace Period

1. There is no revocation grace period under this CP.

4.9.5 Time within which CA must Process the Revocation Request

1. The CA shall process the revocation request on receipt.

4.9.6 Revocation Checking Requirement for Relying Parties

1. Relying Parties shall exercise due care before undertaking transactions and should use mechanisms and repositories provided by NBN Co Limited for checking the status of certificates upon which they intend to rely.
2. It is the sole responsibility of a Relying Party to determine, via the Certificate Status Services, that the status of a Certificate is appropriate prior to the Relying Party's use of that certificate.

4.9.7 CRL Issuance Frequency

1. Circumstances related to emergency CRL issuance are specified in Section 4.9.12
2. A Certification Authority that operates off-line must issue and publish CRLs at least once every 12 months.
3. A Certification Authority that operates on-line and signs end-entity certificate requests must issue and publish CRLs at least once every 30 days.
4. CRL's may be issued and published more frequently than the issuance frequency defined above.
5. CRL's shall be published not later than the next scheduled update.
6. All CRL's are published in accordance with Sections 2.2 and 4.9.8

4.9.8 Maximum Latency for CRLs

1. CRLs shall be published within four (4) hours of generation or no later than the time specified in the next update field of the previously issued CRL for same scope which ever will occur first.

4.9.9 On-Line Revocation/Status Checking Availability

1. CAs may optionally support on-line status checking.
2. If the Certificate Status Services include online CRLs, the location of the CRL shall be encoded in the appropriate Certificate extension.
3. If the Certificate Status Services include Online Certificate Status Protocol (OCSP), the location of the OCSP responder shall be encoded in the appropriate Certificate extension.

4.9.10 On-Line Revocation Checking Requirements

1. It is the sole responsibility of a Relying Party to determine which, if any, on-line Certificate Status Services are used.
2. Relying Parties using on-line revocation checking where this is supported need not obtain or process CRLs.
3. Relying Parties must conform Section 6.3 'CRL Validation' of RFC 5280 when validating the revocation.

4.9.11 Other Forms of Revocation Advertisements Available

1. There are no other forms of revocation advertisements available under this CP.

4.9.12 Special Requirements Related to Key Compromise

1. If a certificate is lost or it is suspected that the Private Key is compromised, a new CRL containing the revoked certificate must be published within 24 hours of revocation.
2. In an event or suspected or actual CA key compromise the **NBN** Co PKIPA, will assess the situation and determine the appropriate course of action to confirm and address the compromise. If deemed necessary, nbn shall use commercially reasonable efforts to notify potential Relying Parties if **NBN** Co PKIPA discovers, or has reason to believe, that there has been a compromise of a CA private key.
3. This CP makes no stipulation as to the total time elapsed from notification of a Private Key compromise to revocation of the certificate.

4.9.13 Circumstances for Suspension

1. Suspension of certificates is not allowed under this policy.

4.9.14 Who Can Request Suspension

1. Not applicable.

4.9.15 Procedure for Suspension Request

1. Not applicable.

4.9.16 Limits on Suspension Period

1. Not applicable.

4.10 Certificate Status Services

1. All CAs shall provide CRLs. CAs may optionally support On-line Certificate Status Protocol (OCSP). The NBN Co PKI does not support any other certificate status services.

4.10.1 Operational Characteristics

1. CRLs shall be available via at least one of HTTP, FTP or LDAP.
2. OCSP Responders shall function in a manner that ensures that revocation status responses provide authentication and integrity services commensurate with the Assurance Level of the certificate being checked.
3. Delta CRLs may be used where the current CRL for a CA becomes too large.
4. Revocation codes that may be used are in accordance with RFC 5280.

4.10.2 Service Availability

1. The current CRL shall always be available from the repository, with frequency and latency as given in Sections 4.9.7 and 4.9.8
2. OCSP Responders shall function in a manner that ensures that accurate and up-to-date information from the authorised CA is used to provide the revocation status.

4.10.3 Optional Features

1. No Stipulation.

4.11 End of Subscription

1. The Subscriber shall indicate the end of subscription by initiating the revocation of their certificates in accordance with Section 4.9

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

1. No copy of any High Assurance or Medium Assurance Authentication/Signature Private Key shall be held by any entity other than the Subscriber. This is particular to Authentication and Signature purposes.
2. A High Assurance Authentication/Signature Private Key shall not be used for confidentiality encryption.
3. A High Assurance Authentication/Signature Private Key cannot be recovered by the CA. If lost or corrupted, new keys must be generated and a new certificate issued.
4. Backup and recovery of confidential Private Keys shall primarily be the responsibility of the Subscriber.
5. Where the Subscriber is internal to NBN Co PKI or in any case where the data to be encrypted shall remain the responsibility of the NBN Co Limited, copies of Confidentiality Private Keys shall also be secured by the CA or delegated RA to ensure recovery of data in the event of loss or damage of the Subscriber's keys.
6. Copies of the CA certificates (containing the Public Key) shall be stored in the repository, published and replicated as required to provide utility and availability.
7. Requests for Key Escrow will be excepted from the following parties only:
    a. From the Subscriber, if the Subscriber has lost or damaged the private-key token,
    b. From the Subscriber's organisation, if the Subscriber is not available or is no longer part of the said organisation,
    c. From an authorised investigator or auditor, if the Private Key is part of a required investigation or audit,
    d. From a requester authorised by a competent legal authority to access the communication that is encrypted using the key,
    e. From a requester authorised by law or governmental regulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

1. Session Key recovery is not supported under this CP.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

1. All CAs and RAs operating under this CP shall operate with physical and environmental security controls appropriate to the Certificate Assurance Levels of the Certificates issued.

5.1.1 Site Location and Construction

1. All CAs and RAs operating under this CP shall be housed in secure facilities.

5.1.2 Physical Access

1. Equipment used to host CAs, and RAs shall be protected from unauthorised access. The Certification Authority Manager (CAM) shall implement physical access controls.

5.1.3 Power and Air Conditioning

1. All critical components shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

1. The secure facilities of the CAs and RAs shall be protected against water exposure.

5.1.5 Fire Prevention and Protection

1. The secure facilities housing the CAs, and RAs shall provide normal fire prevention and protection measures, in line with local applicable safety regulations.

5.1.6 Media Storage

1. All media containing sensitive PKI information, including security audit, archive, or backup information, shall be stored in a location separate from the secure facilities housing the CA and RA equipment, of at least equivalent security to the facilities housing the CA and RA equipment.

5.1.7 Waste Disposal

1. Sensitive information shall not be compromised through the waste disposal procedures.

5.1.8 Off-Site Backup

1. System backups, sufficient to recover from system failure, shall be made on a periodic schedule.
2. One copy of the Backup shall be stored at an off-site location with physical and procedural controls commensurate to that of the operational CA.
3. Requirements for CA Private Key Backup are specified in Section 6.2.4

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 Certification Authority Owner

1. The Certification Authority Owner (CAO) is the legal entity responsible for the CA.
2. The CAO has responsibility for:
    a. establishing the Policy Authority (PA),
    b. ensuring that the appointment of all personnel to Trusted Roles is performed in accordance with Section 5.3
    c. notifying all PKI Participants of an intention to terminate the CA, and
    d. complying with Privacy requirements in accordance with Section 9.4

5.2.1.2 Policy Authority

1. The Policy Authority (PA) is the entity responsible for the approval of CA policies.
2. The PA has responsibility for:
    a. ensuring compliance with requirements set out by NBN Co Limited, and
    b. ensuring compliance with NBN Co Limited policy directions.
3. The PA has responsibility for approval of:
    a. the establishment of the CA,
    b. the appointment of the CAM,
    c. this CP,
    d. the associated CPS,
    e. Subscriber Agreements, and
    f. Relying Party Agreements.
4. The PA may appoint a PA Technical Advisory Group to assist it in meeting its obligations and responsibilities.

5.2.1.3 Certification Authority Manager

1. The Certification Authority Manager (CAM) is the individual responsible for overseeing the management and operation of their respective CA. A CAM is required for each CA, and the same individual may function as CAM for multiple CAs.
2. The CAM has responsibility for ensuring that their respective CA:
    a. complies with the requirements set out by the NBN Co PKIPA,
    b. complies with the requirements of the Subscriber Agreement with the CA that issued the CA-certificate, and
    c. complies with the conditions and obligations set out in this CP and the CPS.
3. In particular, the CAM shall have responsibility for:
    a. ensuring that the generating, issuing, and revocation of Certificates occurs in accordance with this CP and the CPS including:
        i. Certificate profile requirements in accordance with Section 7.1
        ii. CRL profile requirements in accordance with Section 7.2 and
        iii. OCSP profile requirements in accordance with Section 7.3
    b. ensuring that, at the time Certificates are signed and returned to the Subscriber or RA:

i. the Certificates accurately reflect the information provided to the CA by the Subscriber or RA, and
ii. the Certificates contain all the elements required by the Certificate profile.

c. ensuring that appropriate access controls are maintained on the Repository in accordance with Section 2.4
d. ensuring that the CA receives Revocation requests for Certificates and takes appropriate action,
e. ensuring that physical access controls are implemented in accordance with Section 5.1
f. authorising audits,
g. ensuring that the CA conducts and participates in regular audits,
h. ensuring that procedures are implemented for handling security Audit data in accordance with Section 5.4
i. appointment of all Trusted Roles in accordance with Section 5.3
j. acting as the custodian of CA and RA archived data and ensuring that data archived is in accordance with Section 5.5
k. ensuring that procedures are implemented for handling compromise and disaster recovery in accordance with Section 5.7
l. ensuring that no Certificate requests are signed by the CA once the CA has been terminated, and
m. ensuring that the Subscriber Agreement contains:
i. Private Key requirements in accordance with Sections 3.2.1 6.1.1 and 6.2.1
ii. acknowledgement of Certificate acceptance in accordance with Section 4.4.1
iii. Private Key Backup, recovery, and escrow requirements in accordance with Sections 4.5.1 4.12.1 and 6.2.4
iv. agreement to use Private Key for Permitted Uses in accordance with Section 4.4.1
v. Private Key compromise reporting time frames commensurate with the appropriate Certificate Assurance Level in accordance with Sections 4.9.4 and 4.9.12
vi. the process to indicate end of Subscription to the CA in accordance with Section 4.11
vii. acceptance of transferred liability in accordance with Section 9.6
viii. consent to the collection of Personal Information in accordance with the Subscriber Agreement and Section 9.4
ix. acknowledgement of intellectual property rights in accordance with Section 9.5 and
x. an indemnity in favour of the CAO.

4. Where the responsibilities of a role identified in this CP are delegated to a system rather than an individual, the CAM shall ensure that the system meets the requirements of that role.

5.2.1.4 Registration Authority Manager

1. The Registration Authority Manager (RAM) is the individual responsible for overseeing the management and operation of a RA where a CA has delegated these duties to one or more RAs. A RAM is required for each RA. The same individual may function as RAM for multiple RAs.
2. The RAM has responsibility for ensuring that their respective RA:
    a. complies with the requirements set out by the NBN Co PKIPA, and
    b. complies with the conditions and obligations set out in this CP and the CPS.
3. In particular, the RAM shall have responsibility for:
    a. ensuring enrolment and registration procedures are completed in accordance with the requirements of this CP and the CPS,

b. ensuring the identity of Subscribers is verified and validated as part of the authentication requirements as governed by this CP and the CPS,
c. ensuring that the issuance, use, revocation, and re-issuance of credentials meets the requirements of this CP and the CPS, and
d. conducting and participating in regular audits

5.2.1.5 Registration Officer

1. The RO is responsible for the routine operation of the RA including:
    a. ensuring Subscribers comply with the Certificate Application requirements,
    b. verifying the identity of Subscribers,
    c. enrolling and maintaining Subscribers in the PKI,
    d. requesting and executing the issuance of certificates,
    e. verifying the accuracy of information included in certificates,
    f. requesting and executing the revocation of certificates, and
    g. notifying a Subscriber of certificate issuance and revocation.

5.2.1.6 Authorised Officer

1. The AO is responsible for maintaining the integrity of certificate issuance including:
    a. approving the issuance of certificates, and
    b. requesting or approving the revocation of certificates
2. An AO cannot approve issuance of their own certificate.

5.2.1.7 Auditor

Security Auditor

1. The Security Auditor role shall be responsible for:
    a. reviewing, maintaining, and archiving Audit logs, and
    b. performing vulnerability assessments in accordance with Section 5.4.8

Compliance Auditor

1. The Compliance Auditor role shall be responsible for:
    a. performing or overseeing internal compliance audits to ensure that the CA and associated RAs are operating in accordance with this CP and the CPS.

5.2.1.8 Off-line HSM Custodian

1. The Off-Line HSM Custodian role shall only exist where an Off-line HSM is used.
2. The Off-Line HSM Custodian shall be responsible for the physical security of a HSM when not in legitimate use.
3. The Off-Line HSM Custodian cannot have User access to the Keys in the HSM(s) under their control.

5.2.1.9 HSM Security Officer

1. The HSM Security Officer role shall be responsible for:
    a. initialisation, configuration, and activation of a HSM for use, and
    b. establishing and maintaining HSM Operators and HSM Users.

5.2.1.10 HSM Operator

1. The HSM Operator shall be responsible for:
    a. establishing and maintaining a HSM operational environment, and
    b. managing HSM backups and recovery.

5.2.1.11 HSM User

1. The HSM User role shall be responsible for:
    a. generating Keys in the HSM, and
    b. using Keys in the HSM

5.2.1.12 Operator

1. The Operator role shall be responsible for the routine operation of the CA or RA equipment and operations such as system backups and recovery.

5.2.1.13 System Administrator

1. The System Administrator role shall be responsible for:
    a. installation, configuration, and maintenance of the CA or RA,
    b. establishing and maintaining system accounts,
    c. configuring Certificate profiles or templates, and
    d. configuring system Audit parameters.

5.2.1.14 Escrow Officer

1. The Escrow Officer (EO) shall be responsible for:
    a. secure escrow of Private Keys,
    b. recovery of Escrowed Keys, and
    c. validation of recovery requests.

5.2.2 Number of Persons Required for Task

1. Multi-person control shall be in accordance with Section 6.2.2

5.2.3 Identification and Authentication for Each Role

1. All people assigned to a Trusted Role require NBN Co PKIPA approval and must have met the Identification requirements necessary to meet the medium Assurance Level, as defined in Section 1.4.1 prior to being appointed to the trusted role/s.

5.2.4 Roles Requiring Separation of Duties

1. Procedural controls shall be in place to ensure separation of duties between the Registration Officers, Authorising Officer and Certification Authority Administrators.
2. Split-knowledge systems or key-splitting techniques may be used.
3. An Auditor shall not hold any other role with a CA for which they hold an Auditor role.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

1. All people appointed to a Trusted Role:
    a. are Subject to the terms and conditions that apply to their employment or contract arrangement.
    b. should have qualifications and experience commensurate with the functions and responsibilities for the roles defined in this CP.
    c. should be appointed in writing by the NBN Co PKIPA or be party to a contract for PKI services.

5.3.2 Background Check Procedures

1. No Stipulation.

5.3.3 Training Requirements

1. The NBN Co PKIPA is responsible for providing training to people filling NBN Co PKI related roles and may authorise PKI related training to any party including:
    a. people appointed to Trusted Roles,
    b. members of the NBN Co PKIPA,
    c. people from external organisations that support the NBN Co PKI,
    d. any other member of NBN Co Limited determined by the NBN Co PKIPA.

5.3.4 Retraining Frequency and Requirements

1. Any notable change to facility, management, or operational controls shall result in the development of an appropriate training and/or awareness plan.

5.3.5 Job Rotation Frequency and Sequence

1. No Stipulation.

5.3.6 Sanctions for Unauthorised Actions

1. The CAO shall undertake appropriate administrative and disciplinary actions against personnel appointed to trusted roles who violate this CP.

5.3.7 Independent Contractor Requirements

1. The CAO shall ensure that any independent contractors or subcontractors involved in the provision or operation of the Certification Authority are bound to the obligations specified in the CPS and this CP.

5.3.8 Documentation Supplied to Personnel

1. Personnel appointed to Trusted Roles shall have access to documentation and materials sufficient to enable them to meet the obligations and responsibilities of their Trusted Roles.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

1. All PKI related activity logging functions of the systems supporting PKI operations shall be enabled.
2. Each action performed by a Trusted Role is an auditable event.
3. For each auditable event, the Audit record shall include, as applicable:
    a. the type of event,
    b. the date and time the event occurred,
    c. the identity of the trusted role who performed the action,
    d. the success or failure status of the action, and
    e. any associated activity log records for the systems supporting PKI operations.
4. Where possible, the security audit data shall be automatically collected; when this is not possible a logbook, paper form, or other physical mechanism shall be used.

5.4.2 Frequency of Processing Log

1. For High Assurance, at least two periodic reviews are required per year, with at least 33 percent of the security Audit data generated since the last review to be examined.
2. For Standard/Medium Assurance, at least one periodic review is required per year, with a minimum of 10 percent of the security Audit data generated since the last review to be examined.

5.4.3 Retention Period of Audit Log

1. Audit logs shall be retained in accordance with NBN Co Limited record retention policies.

5.4.4 Protection of Audit Log

1. Audit logs shall be secured to prevent:
    a. Modification,
    b. Deletion, and
    c. Unauthorised access.
2. Audit logs may be copied for reporting purposes. The copied Audit logs must retain the integrity of the information contained in the original.

5.4.5 Audit Log Backup Procedures

1. Security Audit data must be backed up.

5.4.6 Audit Collection System (Internal vs. External)

1. The security Audit process shall run independently and shall not in any way be under the control of the CA or RA personnel.
2. Security Audit processes shall be invoked at system start-up and cease only at system shutdown. Should it become apparent that an automated security Audit system has failed, the CA or RA shall cease all operation except for revocation processing until the security Audit capability can be restored.

5.4.7 Notification to Event-Causing Subject

1. No Stipulation.

5.4.8 Vulnerability Assessments

1. The security Audit logs shall be reviewed by the Security Auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. The Security Auditor shall check for continuity of the security Audit logs.

5.5 Records Archival

5.5.1 Types of Records Archived

1. Archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data shall be archived:
    a. For all Assurance Levels:
        i. CA accreditation,
        ii. CPs and CPSs, and
        iii. System equipment configuration.
    b. For Standard/Medium Assurance and High Assurance:
        i. modifications or updates to any of the above items,
        ii. certificate requests and revocation requests,
        iii. Subscriber identity authentication documentation as required by Section 3.2.3
        iv. all certificates and CRLs as issued or published,
        v. security Audit data (in accordance with Section 5.4
        vi. other data or applications sufficient to verify archive contents, and
        vii. all work-related communications to or from compliance auditors.

5.5.2 Retention Period of Archive

1. Records shall be retained in accordance with NBN Co Limited archive approved retention and disposal policies.

5.5.3 Protection of Archive

1. Records shall be protected in accordance with NBN Co Limited archive approved retention and disposal policies.

5.5.4 Archive Backup Procedures

1. Records shall be backed up in accordance with NBN Co Limited archive approved retention and disposal policies.

5.5.5 Requirements for Timestamping of Records

1. No Stipulation.

5.5.6 Archive Collection System (Internal vs. External)

1. No Stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

1. No Stipulation.

5.6 Key Changeover

1. CAs must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and Public Keys.
2. A CA certificate may be re-keyed during the life of the certificate if there is a risk that the CA Private Key could be compromised. If a re-key occurs, only the new key will be used for certificate signing purposes from that time.
3. The older, but still valid, certificate must be available to verify old signatures until all the Subscriber certificates signed under it have also expired or are revoked.
4. If the old Private Key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

1. The CAM shall ensure appropriate incident response procedures are followed for handling incidents that may impact the operation of the CA.

5.7.2 Computing Resources, Software, and/or Data are corrupted

1. The CAM shall ensure that the CA shall have the capability to continue CA operations in case of software and/or data corruption.

5.7.3 Entity Private Key Compromise Procedures

1. In the case of Private Key compromise of an NBN Co CA, the CA certificate shall be revoked.
2. The CAM shall attempt to promptly notify all Relying Parties of the Revocation, in accordance with Section 9.8

5.7.4 Business Continuity Capabilities after a Disaster

1. Medium Assurance and High Assurance CAs are required to maintain an approved Disaster Recovery Plan. Recovery procedures shall be invoked according to the approved Disaster Recovery Plan.

5.8 CA or RA Termination

1. The CAM or RAM must notify the NBN Co PKIPA and all relevant stakeholders if a NBN Co CA or RA is to be terminated, including notification of procedures for the continuance or otherwise of PKI services.
2. When a CA or RA is terminated, the CAM or RA must:
    a. surrender the CA/RA keys.
    b. implement the archival processes defined in Section 5.5

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 NBN Co Certification Authorities

1. Key pairs for NBN Co-signed CAs shall be generated in FIPS 140-2 level 3 or higher Cryptographic modules.
2. The NBN Co PKIPA will approve all requests to generate key pairs for NBN Co-signed CAs. Requests must be made to the NBN Co PKIPA by the CA CAM.
4. Root and Intermediate CA Certificate will have the following restrictions applied to any certificate:
    a. Within the Key Usage (2.5.29.15) OID, only the following values may be set:
        i. Certificate Signing
        ii. CRL Signing
    b. The Path Length Constraint will be not set within the certificate basic constraints.
5. Issuing CA Certificates will be issued with the following constraints:
    a. Within the Key Usage (2.5.29.15) OID, only the following values may be set:
        i. Certificate Signing
        ii. CRL Signing
    b. The Path Length Constraint must be set to 0 within the certificate basic constraints.

6.1.1.2 NBN Co Registration Authorities

1. Key pairs for NBN Co approved RAs shall be generated in FIPS 140-2 level 2 or higher Cryptographic modules.
2. Generation of key pairs for NBN Co approved RAs will be requested by the CAM for the RA.

6.1.1.3 Subscribers

1. Subscriber key pairs for High Assurance certificates must be generated in a FIPS 140-2 level 3 or higher Cryptographic Module that must reside on the Subscriber security device, for example, smart card or token.
2. Subscriber key pairs for Standard/Medium Assurance certificates shall be generated in a FIPS 140-1/2 level 2 software Cryptographic modules (usually web browser certificate cache or another comparable certificate store).
3. Subscriber key pairs for Basic Assurance certificates can be generated in a FIPS 140-1/2 level 2 software Cryptographic modules (usually web browser certificate cache or another comparable certificate store).
4. Subscriber key pairs can be generated by:
    a. the Subscriber
    b. a NBN Co RA
    c. a NBN Co Issuing CA

6.1.2 Private Key Delivery to Subscriber

1. High Assurance key pairs shall be generated locally in a hardware Cryptographic Module by the Subscriber.

2. Private Keys associated with Standard/Medium Assurance and Basic Assurance certificates may be generated and stored in software. When the Subscriber generates these keys locally, there is no need to deliver them. If the Private Keys are generated elsewhere, they must be transmitted or delivered to the Subscriber in encrypted form and the encryption method ensures that only the Subscriber may possess the Plaintext private signature keys. The encryption must be of strength commensurate with that of the key being protected. The Subscriber shall acknowledge receipt of the private signature key. The originally generated private signature key shall be destroyed.
3. Mechanisms shall ensure that additional copies of software keys are not maintained except as allowed in this Certificate Policy.
4. For all Assurance Levels, when keyed hardware tokens are delivered to Subscribers, the delivery shall be accomplished in a way that ensures that the correct tokens and Activation Data are provided to the correct Subscribers. The CA must maintain a record of receipt of the token by the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

1. Public Keys shall be delivered to CA in signed certificate requests.

6.1.4 Key Sizes

1. The NBN Co Root and Intermediate CAs require a minimum RSA key length of 4096 bits.
2. Issuing CAs under an NBN Co Intermediate CA require a minimum RSA key length of 2048 bits.
3. Assurance Level end-entity certificates must have a key length of at least 2048 bits (RSA).
4. All certificate authorities issuing certificates or CRLs must use the SHA-2 hash algorithm for digital signatures.
5. The use of smaller key sizes is only permitted if expressly approved by the PKIPA or its delegate; approval is mandatory in every case where a key size of less than 2048 bits or equivalent-strength algorithms are considered.

6.1.5 Public Key Parameters Generation and Quality Checking

1. No Stipulation.

6.1.6 Key Usage Purposes (as per X.509 V3 Key Usage Field)

1. The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.
2. In particular:
    a. Certificates used for authentication set the Digital Signature bit,
    b. Certificates used for key encryption set the key Encipherment bit,
    c. Certificates used for data encryption set the data Encipherment bit,
    d. Certificates used for Digital Signatures set the Digital Signature bit,
    e. CA certificates set cRLSign and key CertSign bits,
    f. Certificates used for key agreement set the key Agreement bit.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

1. The relevant standard for Cryptographic modules is “FIPS 140-2 Security Requirements for Cryptographic modules”.

6.2.2 Private Key (m out of n) Multi-Person Control

1. CA Private Key material or other critical information shall be protected by multi person controls.

6.2.3 Private Key Escrow

1. CA Private Keys shall not be escrowed.
2. Subscriber Private Key Escrow shall be in accordance with Section 4.12.1

6.2.4 Private Key Backup

1. High Assurance Private Keys shall only be backed up within hardware cryptographic modules.
2. Subscribers are permitted to make operational copies of Private Keys residing in software for each of the Subscriber’s applications or locations that require the key in a different location or format.
3. RAs shall not back-up Private Keys.
4. Backup copies of CA private signature keys shall only be made and handled under the same multi-person control as the original signature key. If backups are made, at least one copy shall be kept at a backup location.

6.2.5 Private Key Archival

1. Refer to Sections 6.2.4 and 6.2.5

6.2.6 Private Key Transfer into or From a Cryptographic Module

1. High Assurance Private Keys shall never be transferred from a hardware cryptographic module. Such keys shall only be transported within a hardware cryptographic module or backed up by out-of-band duplication of the hardware cryptographic module itself.
2. If a Private Key is to be transported, the Private Key must be encrypted during transport and the strength of the encryption must be at least commensurate with the key being transported.

6.2.7 Private Key Storage on Cryptographic Module

1. Refer to Section 6.2.1

6.2.8 Method of Activating Private Key

1. Passphrases, PINs, biometric data, or other mechanisms of equivalent authentication robustness must be used to activate the Private Key that is stored in a cryptographic module.

6.2.9 Method of Deactivating Private Key

1. Cryptographic modules, which have been activated, must not be left unattended or otherwise open to unauthorised access.
2. After use, they must be deactivated, via a manual logout procedure, or by a passive timeout.

6.2.10 Method of Destroying Private Key

1. The CAM shall ensure that CA and RA private signature keys are destroyed when they are no longer needed.
2. Cryptographic Module Operator Token Holders shall surrender their Cryptographic Module tokens to CA/RA personnel or trusted agents for destruction when they are no longer needed. Physical destruction of the Hardware Security Module (HSM) is not required. The HSM tokens may be destroyed.
3. The CAM, RAM or Registration Officer shall destroy a Subscriber Digital Signature Private Keys when no longer required.

6.2.11 Cryptographic Module Rating

1. See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

1. The Public Key shall be archived as part of the Certificate archival in accordance with Section 5.5.1

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

1. The maximum NBN Co PKI CA certificate and key lifetimes are given as a function of key-size and level of assurance as follows:

Table 2 - Maximum Key Lifetimes

Modulus Size	High Assurance	Medium Assurance	Basic Assurance
2048 bits	10 years	15 years	20 years
3072 bits	25 years	30 years	35 years
4096 bits	40 years	40 years	40 years

2. The maximum key lifetime period for any issued certificate is 2 years.
3. The maximum key lifetime may be prescribed to be shorter for some key usage due to the following:
    a. Large data flow or number of transactions utilising said key,
    b. Security life of the data,
    c. Number of nodes using the same key,
    d. The number of copies or distribution of the key, or
    e. A security requirement.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

1. Activation data may be Subscriber selected.
2. A passphrase, PIN, biometric data, or other mechanisms of equivalent authentication robustness shall be used to protect access to use of a Private Key.

6.4.2 Activation Data Protection

1. Activation data for cryptographic modules shall be secured at the level of the data that the associated cryptographic module is used to protect and shall not be stored with the cryptographic module.
2. Activation data for Private Keys associated with certificates asserting individual identities shall never be shared.
3. Activation data for Private Keys associated with certificates asserting organisational identities shall be restricted to those in the organisation authorised to use the Private Keys.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

1. No Stipulation.

6.4.3.2 Activation Data Destruction

1. No Stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

1. The NBN Co CA equipment shall use operating systems that:
    a. require authenticated logins,
    b. provide discretionary access control,
    c. provide a security audit capability, and
    d. meet the terms and conditions of the nbn Public Key Infrastructure - Certificate Policy (this document).

6.5.2 Computer Security Rating

1. No Stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

1. System development controls shall be in accordance with Section 6.6.1 (System Development Controls) of the CPS.

6.6.2 Security Management Controls

1. Security management controls shall be in accordance with Section 6.6.2 (Security Management Controls) of the CPS.

6.6.3 Lifecycle Security Controls

1. Lifecycle security controls shall be in accordance with Section 6.6.3 (Life Cycle Security Controls) of the CPS.

6.7 Network Security Controls

1. Network security controls shall be in accordance with Section 6.7 (Network Security Controls) of the CPS.

6.8 Timestamping

1. Time stamping shall be in accordance with Section 6.8 (Timestamping) of the CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

1. All Certificates shall be X.509 version 3 Certificates.
2. All CRLs shall be X.509 version 2 CRLs.

7.1.1 Version Number(s)

1. Certificates shall conform to the IETF PKIX, RFC 5280.

7.1.2 Certificate Extensions

1. The issuer UniqueId extension shall not be used.
2. The SubjectUniqueId extension shall not be used.
3. The authority KeyIdentifier extension is not required in the NBN Co Root CA certificate.
4. The authority KeyIdentifier extension shall be included in all other certificates issued under this CP.
5. The Subject KeyIdentifier extension shall be included in all CA certificates issued under this CP.
6. The SubjectKeyIdentifier extension should be included in all other Certificates issued under this CP.
7. The key Identifier field shall be derived by either method (1) or method (2) under RFC 5280.
8. The Certificate Policies extension should not be used in the NBN Co Root CA certificate.
9. The authority InfoAccess extension may be included in Certificates issued under this CP.
10. The Subject InfoAccess extension may be included in Certificates issued under this CP.

7.1.3 Algorithm Object Identifiers

1. Certificates issued by the CAs under this CP shall identify the signature algorithm using these OIDs:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3}

2. The algorithm SHA-1 must not be used for new certificates as of the publication of this document. A larger algorithm must be used, unless at the approval of the PKIPA.

7.1.4 Name Forms

1. CA certificates shall not have an empty Subject name.
2. DNs may contain the domain Component attribute, as defined in RFC 4519.
3. All DNs shall contain a minimum of one non-domain Component (DC) RDN or at least two domain Component (DC) RDNs.
4. DNs shall comply with RFC 5280 and RDNs shall be sequenced, in accordance with X.501.

7.1.5 Name Constraints

1. No Stipulation.

7.1.6 Certificate Policy Object Identifier

1. Certificates issued under this policy shall assert the OID appropriate to the level of assurance with which it was issued, as defined in Section 1.2.1

7.1.7 Usage of Policy Constraints Extension

1. No Stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

1. In an End Entity Certificate the OID asserted in accordance with Section 7.1.6 shall have a CPS Pointer qualifier containing a URI referring to the issuing CA's Repository.
2. In a CA certificate the OID asserted in accordance with Section 7.1.6 shall have a CPS Pointer qualifier containing a URI referring to the Subject CA's Repository.
3. The OID asserted in accordance with Section 7.1.6 shall have a User Notice qualifier containing an explicit Text field with the content "Issued under NBN Co PKI. Refer to and https://pki.nbnco.net.au/ for more information."
4. The OID asserted in accordance with Section 7.1.6 shall have a User Notice qualifier containing an explicit Text field with the content "Certificates issued for NBN Co Private <<NBN Co Environment>> Use."

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

1. No Stipulation.

7.2 CRL Profiles

1. CRLs shall confirm to the IETF PKIX, RFC 5280.

7.2.1 Version Number(s)

1. The version shall be 2 of which is denoted as a 1 in the Version field.

7.2.2 CRL and CRL Entry Extensions

1. The authority KeyIdentifier extension shall be included in all CRLs.
2. The cRLNumber extension shall be included in all CRLs.

7.3 OCSP Profiles

7.3.1 Version Number(s)

1. OSCP version 1 shall be used.

7.3.2 OCSP Extensions

1. Appropriate extensions from RFC 2560 may be used in OCSP requests and responses.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

1. Assessments required to be conducted in accordance with this CP shall be performed on an annual basis.

8.2 Identity/Qualifications of Assessor

1. External auditors engaged by NBN Co Limited to assess the NBN Co PKI will be selected from the NBN Co PKIPA.
2. The NBN Co Internal Auditor may be used to conduct NBN Co PKI assessments.
3. The NBN Co PKIPA will be responsible for auditing the NBN Co Root CA and NBN Co Intermediate CAs.

8.3 Assessor's Relationship to Assessed Entity

1. The internal or external auditors must not hold any other Trusted Role in the NBN Co PKI.

8.4 Topics Covered by Assessment

1. The topics to be covered by the Accreditation Audit of the NBN Co PKI are:
    a. compliance of the NBN Co PKI with the NBN Co requirements for an annual Audit,
    b. CP changes,
    c. CPS changes,
    d. compliance of the NBN Co Issuing Certification Authorities with the nbn Public Key Infrastructure - Certificate Policy (this document),
    e. compliance of the NBN Co Registration Authorities with the nbn Public Key Infrastructure - Certificate Policy (this document),
    f. compliance of the NBN Co Issuing Certification Authorities with its Certification Practice Statement, and
    g. security breaches, compromises, and mitigation.

8.5 Actions Taken as a Result of Deficiency

1. The NBN Co PKIPA must consider all recommendations arising from an Audit assessment.
2. The CAM for an Issuing CA is responsible for addressing any serious deficiencies in a timely manner.
3. The NBN Co PKIPA must take timely and appropriate action to ensure the NBN Co PKI does not compromise the NBN Co PKI.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

1. Fees may be payable by Subscribers for the issue or renewal of certificates. Where fees are payable, details will be set out in the relevant agreements or other documentation and an up-to-date fee schedule shall be provided to Subscribers by way of a Notice in accordance with Section 9.8

9.1.2 Certificate Access Fees

1. Fees may be payable for Certificate access. Where fees are payable, details will be set out in the relevant agreements or other documentation and an up-to-date fee schedule shall be provided by way of a Notice in accordance with Section 9.8

9.1.3 Revocation or Status Information Access Fees

1. Fees may be payable by Subscribers for Revocation or reversal of Suspension of a Certificate, or for access to the Certificate Status Services. Where fees are payable, details will be set out in the relevant agreements or other documentation and an up-to-date fee schedule shall be provided by way of a Notice in accordance with Section 9.8

9.1.4 Fees for Other Services

1. No Stipulation.

9.1.5 Refund Policy

1. A refund policy may apply to any fees levied in accordance with Section 9.1 Where a refund policy applies, details will be set out in the relevant agreements or other documentation, and it shall be documented in the fee schedule.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

1. It is the sole responsibility of each PKI Participant to determine the appropriate insurance coverage in regard to any liability, claims, loss or damage (and any associated costs or expenses) that may be suffered or incurred as a result of using a Certificate or associated Keys issued under this CP.

9.2.2 Other Assets

1. No Stipulation.

9.2.3 Insurance or Warranty Coverage for End Entities

1. Each PKI Participant acknowledges that the CAO does not provide any insurance coverage or warranty for the benefit of PKI Participants in relation to any liability, claims, loss or damage (and any associated costs or expenses) that may be suffered or incurred as a result of participating in the Certificate application process or using a Certificate or associated Keys issued under this CP.

9.3 Confidentiality

9.3.1 Scope of Confidential Information

1. The CAO may receive Confidential Information from PKI Participants while fulfilling its functions under this CP.
2. Subject to Section 9.3.2 Confidential Information means, in relation to a PKI Participant, information that is not trivial and that:
    a. is by its nature confidential,
    b. is communicated by the PKI Participant to the CAO and in a way as being identified as confidential, and
    c. the CAO knows or ought to know is confidential.

9.3.2 Information Not Within the Scope of Confidential Information

1. Notwithstanding Section 9.3.1 Confidential Information does not include information which:
    a. was already lawfully disclosed by the CAO prior to the CAO being required to treat the information as confidential,
    b. is lawfully received from a third party who is not bound by a duty of confidentiality,
    c. has become public knowledge, other than through a breach of an obligation of confidence under this CP,
    d. was independently developed or released by the CAO without reference to the Confidential Information,
    e. is information that the PKI Participant provides for inclusion within a Certificate,
    f. is information indicating that a Certificate has been Revoked or Suspended, though not including the reason behind this Certificate Status, or
    g. includes any information relating to the PKI Participant's use of the Repository.

9.3.3 Responsibility to Protect Confidential Information

1. Subject to Section 9.3.3 paragraph 2, the CAO shall protect any Confidential Information provided by a PKI Participant in accordance with its usual business practices, any relevant contractual undertakings and any applicable law, and shall not, without the prior written approval of the relevant PKI Participant (which approval shall not be withheld or delayed unreasonably), make public or disclose to any person, the PKI Participant's Confidential Information.

2. Nothing within Section 9.3.3 paragraph 1 shall be construed to prevent the CAO from disclosing any information provided by a PKI Participant:
    a. to any Minister or to Parliament in connection with the conducting of any functions, duties, powers, and discretions conferred on the CAO,
    b. to such legal advisors, financial advisers, auditors, or insurers of the CAO as may be necessary for any proceedings or investigation involving the CAO, or for the purposes of facilitating the CAO's performance of its functions under this CP,
    c. to its personnel and to other government agencies to the extent reasonably required by the CAO in order to perform its duties or obligations under this CP or a Subscriber Agreement or Relying Party Agreement, or
    d. to the extent required by law (including any applicable rules or regulations and the FOI Act referred to in Section 9.3.4 below), a court or tribunal or government policy).

9.3.4 Right to Information and Disclosure

1. The *Freedom of Information Act 1982* (FOI Act) provides members of the public with a general right of access to documents held by NBN Co Limited and its related bodies corporate. The general right of access is subject to a number of exceptions set out in the FOI Act.
2. As a result of the operation of the FOI Act, information provided by or relating to (or both) a PKI Participant (including Confidential Information) may be subject to disclosure to third parties. Further details are set out at: https://www.nbnco.com.au/corporate-information/about-nbn-co/freedom-of-information
3. Notwithstanding any other provisions of this CP or any other document or agreement:
    a. the CAO does not make any representations or warranties that information provided by the PKI Participant will be protected from disclosure under the FOI Act
    b. to the maximum extent permitted by law, a disclosure of information by NBN Co Limited or its related bodies corporate pursuant to the FOI Act will not constitute a breach of any obligation by NBN Co Limited or its related bodies corporate (whether under this CP, another document or agreement, or at law), and
    c. the CAO is entitled to publish the information about the PKI Participant that is contained within a Certificate or related to the PKI Participant's use of the Repository.

9.4 Privacy

9.4.1 Privacy Plan

1. The privacy policy of the CAO, NBN Co Limited, is set out at: https://www.nbnco.com.au/utility/privacy-policy as updated from time to time.
2. The Privacy Policy operates in conjunction with all applicable privacy legislation and regulations, this CP and any relevant agreements entered into by the PKI Participants, in relation to PKI Participant dealings with the CAO pursuant to this CP.
3. "Personal Information" has the meaning given in the NBN Co Limited Privacy Policy.

9.4.2 Information Not Treated as Private

1. Notwithstanding any other provisions within Section 9.4 , the following information is not and will not be treated as being Personal Information for the purposes of this CP and the Privacy Policy:

a. any information contained within a Certificate, Certificate directory or online CRL; and
b. any information relating to PKI Participant's use of the Repository.

and each PKI Participant consents to such information being used and disclosed to the public in accordance with this CP.

9.5 Intellectual Property Rights

1. Except for any Intellectual Property Rights referred to in paragraph 4 below or as otherwise agreed in writing between the PKI Participants, all Intellectual Property Rights subsisting in or relating to any materials created in relation to the NBN Co PKI including any modifications or adaptations ("NBN Co PKI Materials") are owned or licensed by NBN Co Limited including without limitation:
    a. all Certificates, Keys, and related materials,
    b. all related documentation including, without limitation, this Certificate Policy,
    c. Certification Practice Statements, Subscriber Agreements and Relying Party Agreements; and
    d. all other documentation produced in connection the NBN Co PKI.
2. Subscribers and Relying Parties hereby assign on creation any rights including Intellectual Property Rights they may have in any NBN Co PKI Materials.
3. NBN Co grants to Subscribers and Relying Parties a revocable, non-transferable, non-exclusive, royalty-free, personal licence to use the NBN Co PKI Materials to the extent required by Subscribers and Relying Parties in order to participate in the NBN Co PKI.
4. A Certificate Applicant will retain all Intellectual Property Rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and Distinguished Name within any certificate issued to such Certificate Applicant and the Certificate Applicant grants to NBN Co a royalty free, non-exclusive licence to use such Intellectual Property Rights for the purposes of the NBN Co PKI.

9.6 Representations and Warranties and Liability

1. To the maximum extent permitted by law, and except to the extent set out in this Certificate Policy, NBN Co Limited makes no representations or warranties, express or implied, with regard to any aspect of the NBN Co PKI including without limitation:
    a. any Key or Certificate,
    b. any matter referred to or contemplated under this Certificate Policy or any other related documentation (including, without limitation, any related CPS), or
    c. any products or services that may be related or ancillary to, or otherwise used in the delivery of, the NBN PKI.
2. To the maximum extent permitted by law, neither NBN Co or its related bodies corporate (or any of their respective personnel) will be liable to any third party as a result of any claims arising in relation to, or otherwise connection with, the NBN PKI (whether in contract, tort, statute, equity or otherwise) including, without limitation, in respect of:
    a. any Key or Certificate,
    b. any matter referred to or contemplated under this CP or any related CPS, or
    c. any products or services that may be related or ancillary to or otherwise used in the delivery of the NBN PKI.

9.7 Term and Termination

9.7.1 Term

1. This CP, in its entirety, and all Certification Practice Statements, shall remain in force for the life of the NBN Co PKI unless superseded or otherwise terminated by NBN Co in accordance with Section 9.7.2
2. This CP becomes effective when approved by the NBN Co PKIPA.

9.7.2 Termination

1. This CP may be immediately terminated at any time by NBN Co.

9.7.3 Effect of Termination and Survival

1. The requirements of this CP remain in effect through to the end of the archive period for the last certificate issued.
2. Upon termination of this CP, the issuance and generation of further certificates under this CP will cease.

9.8 Individual Notices and Communications with Participants

1. The NBN Co PKIPA shall establish appropriate procedures for communications with parties operating under this policy, as applicable.

9.9 Amendments

9.9.1 Procedure for Amendment

1. The NBN Co PKIPA shall review this CP periodically. Any corrections, updates, or changes to this CP, as determined by NBN Co, shall be publicly available.
2. Third party proposals for change to this CP may be provided to the NBN Co contact listed in Section 1.5.2 The proposals must include:
    a. detailed description of the change,
    b. change justification, and
    c. contact information for the person requesting the change.
3. The NBN Co PKIPA may, but is not obligated to, consider any proposals for change.
4. The NBN Co PKIPA must approve and accept any proposed change to this CP before it is included in this CP.

9.9.2 Notification Mechanisms and Period

1. Amendments to this CP may be posted to the CP URL identified in Section 1.2
2. The amendments, or the modified CP, may be distributed electronically to NBN Co PKIPA participants.

9.9.3 Circumstances under Which OID Must Be Changed

1. A new OID is required if this policy introduces a new Assurance Level.

9.10 Governing Law

1. This CPS is governed by, and is to be construed in accordance with, the laws from time to time in force of the State of New South Wales, Australia. In relation to the CPS and any related matters, each of the PKI Participants irrevocably submit to the non-exclusive jurisdiction of courts having jurisdiction in the State of New South Wales, Australia, and waive any right to object to the venue on any ground.

9.11 Compliance with Applicable Law

1. All Parties agree to abide by the provisions of all relevant legislation, and the requirements of any Commonwealth, State, Territory, or local government agency when conducting activities under this CP.

Appendix A Definitions and Acronyms

Abstract Syntax Notation (ASN.1)	An abstract notation for structuring complex data objects.
Activation Data	Data values, other than keys, which are required to operate Cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually held key share).
Administrator (PKI)	A Trusted Person within the organisation of a Processing Centre that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Application Software Vendor	A developer of Internet browser software or other software that displays or uses Certificates and distributes root Certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
Assurance Level	A specified level of assurances as defined within the CP.
Asymmetric Cryptography	A class of Cryptography in which a Key Pair is used – a Private Key to create signatures and to decrypt messages, and a Public Key to encrypt messages and verify signatures. It has two main advantages: For n users, only n Key Pairs are needed; and Public Keys can be widely distributed with no requirement for confidentiality; but most methods which can achieve good security require significant computing resources. (See Symmetric Cryptography).
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Authorised Party	(Certificate purpose) An Individual or Device with authority to conduct certain actions or make certain assertions.
Authorisation	The granting of rights, including the ability to access specific information or resources.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrolment information matches information contained in a database.
Automated Administration Software Module	Software provided by NBN Co that performs Automated Administration.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.

Business Day	Any day other than a Saturday, Sunday, or public holiday (including public service holidays) for the whole of NBN Co.
CA-Certificate	A Certificate for a CA's Public Key.
Certificate	See X.509 Certificate.
Certificate Applicant	An individual or organisation that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorised agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy compliance Audit.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.
Certificate Profile	The specification of the fields to be included in a Certificate and the contents of each, as set in the relevant Certificate Policy.
Certificate Re-key	Within the NBN Co PKI, Certificate Re-key is defined as the issuance of a new Certificate to replace an existing valid Certificate, with a new serial number, validity, and Public Key, but with no other Subscriber information changed.
Certificate Renewal	Within the NBN Co PKI, Certificate Renewal is defined as the issuance of a new Certificate to replace an existing valid Certificate, with a new serial number and extended validity but with no other Subscriber information changed.
Certificate Revocation List (CRL)	A signed, time-stamped list of serial numbers of the Public Key Certificates of Subscribers (other than Certification Authorities) that have been revoked prior to their scheduled Expiry.
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorised to issue, manage, revoke, and renew Certificates in the NBN Co PKI.
Certification Authority Manager (CAM)	The CA individual who is responsible for overseeing the management of the CA.

Certification Authority Owner (CAO)	The legal entity responsible for the Certification Authority.
Certification Path	An ordered sequence of Certificates that, together with the Public Key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, managing, revoking, and renewing or re-keying Certificates.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrolment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber, and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Ciphertext	Information that has been encrypted into seemingly meaningless code. (See Plaintext).
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorised disclosure of, or loss of control over, sensitive information may have occurred. With respect to Private Keys, a Compromise is a loss, theft, disclosure, modification, unauthorised use, or other compromise of the security of such Private Key.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Cross Certification	The process undertaken by Certification Authorities to establish a trust relationship. When two Certification Authorities are cross-certified, they agree to trust and rely upon each other's Public Key Certificates and keys as if they had issued them themselves. The two Certification Authorities exchange cross-Certificates, enabling their respective users to interact securely.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Device (Certificate)	(Certificate purpose) A device, host, service, or process. For example, a network device, firewall, server, personal computer, handheld digital device, Smartphone, access point, website, service, process, socket, interface, or the like.
Digital Signature	A method of using Cryptography to link an exclusive identity to an electronic document or transaction to accomplish what a written signature accomplishes in a paper document. A Digital Signature also verifies that the contents of the message or document have not been altered.
Distinguished Encoding Rules (DER)	Rules for encoding ASN.1 objects which give a consistent encoding for each ASN.1 value using a binary format.

Distinguished Name (DN)	A unique identifier assigned to each Certificate Applicant, having the structure required by the Certificate Profile.
Dual Use Certificate	A Certificate that is intended for use with both Digital Signature and data encryption services.
Encryption Certificate	A Certificate containing a Public Key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a Session Key for these same purposes.
End Entity	A Relying Party or a Subscriber.
Evidence Of Identity (EOI)	The process implemented to determine the identity of an entity using documents or other information identifying the entity.
Hardware Security Module	A hardware device incorporating tamper protection, used to securely generate and store cryptographic keys.
Hashing	The process of subjecting a set of data to a sequence of mathematical operations to compute a numeric value that will later be compared to ensure the original data has not been altered.
Identification	The process of establishing the identity of an entity, by: • Establishing that a given name of an entity corresponds to a real-world identity of an entity, and • Establishing that an entity applying for or seeking access under that name is, in fact, the named entity.
Intellectual Property Rights	All industrial and intellectual property rights throughout the world, including all copyright and analogous rights, all rights in relation to inventions or discoveries (including patent rights), designs, registered and unregistered trade marks (including service marks), trade names, brand names, indications of source or appellations of origin, know-how, software, circuit layouts and all other rights throughout the world resulting from intellectual activity in the industrial, scientific or artistic fields. These rights include: 1. all rights in all applications to register these rights; and 2. all renewals and extensions of these rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the Root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Issuing Certification Authority (Issuing CA)	In the context of a Certificate, or when the phrase "the issuing CA" is used, the issuing CA is the CA that issued the Certificate. In the context of the NBN Co PKI hierarchy of CAs, or when the phrase "an Issuing CA" is used, an Issuing CA is a CA that issues End-Entity Certificates and does not issue CA-Certificates.
Key	A sequence of symbols that controls the operation of a cryptographic transformation.

Key Escrow	The process of entrusting a Private Key to a third party (an Escrow Agent such as an Organisation or government) and providing another third party with a legal right to obtain the Key from the Escrow Agent in certain circumstances.
Key Exchange	The process of exchanging Public Keys in order to establish secure communications.
Key Generation Ceremony	A procedure whereby a CA's or RA's Key Pair is generated, its Private Key is transferred into a Cryptographic Module, its Private Key is backed up, and/or its Public Key is certified.
Key Pair	A matching Private Key and Public Key which are mathematically linked such that one will decrypt Ciphertext produced with the other. In many cryptosystems, including those used here, the converse is also true, i.e., either key can be used to decrypt Ciphertext produced with the other.
Managed PKI	NBN Co fully integrated managed PKI service that allows enterprise Customers of NBN Co and its Partners to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for a Managed PKI Customer.
Managed PKI Control Centre	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications.
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NBN Co	Means "NBN Co Limited"
NBN Co PKIPA	Means "NBN Co Public Key Infrastructure Policy Authority"
NBN Co PKI Participant	An individual or organisation that is one or more of the following within the NBN Co PKI: NBN Co, a Subscriber, or a Relying Party.
NBN Co PKI Framework	Means "NBN Co Public Key Infrastructure Framework"
NBN Co PKI Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the NBN Co PKI.

NBN Co Repository	NBN Co database of Certificates and other relevant NBN Co PKI information accessible on-line.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a Digital Signature verified with reference to a NBN Co PKI Certificate may provide proof in support of a determination of Nonrepudiation by a tribunal but does not by itself constitute non-repudiation.
No verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Offline CA	NBN Co PCAs, Root CAs and other designated Intermediate CAs that are kept offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are kept online to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a certificate is issued (or on a later date and time certain if stated in the certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of Private Keys.
Plaintext	Information in a directly usable, unencrypted form. (See Ciphertext)
Policy Authority (PA)	The entity responsible for the approval of a Certificate Policy and the associated Certification Practice Statement, Subscriber Agreement and Relying Party Agreement.
Policy Management Authority (PMA)	The organisation within NBN Co responsible for publishing this policy throughout the NBN Co PKI.
Private Key	That Key of an entity's Key Pair which should only be used by that entity and should not be disclosed to any other entity.
Private Signing Key	See Private Authentication Key.

Processing Centre	An organisation (NBN Co or certain other entities) that creates a secure facility housing, among other things, the Cryptographic modules used for the issuance of Certificates.
Public Key	That Key of an entity's Key Pair which can be made public.
Public Key Infrastructure (PKI)	The architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key cryptographic system.
Public-Key Cryptography Standards (PKCS)	A series of cryptographic standards dealing with Public-Key issues, published by RSA Laboratories.
Registration Authority (RA)	An entity which carries out a number of functions on behalf of a Certification Authority (CA), including one or more of the following functions: The Identification and authentication of Certificate applicants, the approval or rejection of Certificate applications and requesting generation of Certificates from the CA, initiating Certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their Certificates, and approving or rejecting requests by subscribers to renew or rekey their Certificates. RAs do not sign or issue Certificates.
Registration Authority Manager (RAM)	The RA individual who is responsible for overseeing the management of the RA.
Registration Information	Information that an applicant is required to disclose for the purpose of obtaining Keys and Certificates.
Relying Party	A recipient of a Certificate which relies on that Certificate for authentication or confidentiality and/or any Digital Signatures verified using that Certificate.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organisation acts as a Relying Party.
Repudiation	The denial or attempted denial of involvement by a party in all or part of an electronic Transaction.
Revoke	The process undertaken by the CA, generally in response to a request by an RA, to invalidate a Certificate. A subscriber may request revocation through the RA.
Root Certification Authority (Root CA)	The CA which is the highest trusted element in the PKI.
Secret Share	A portion of a CA Private Key or a portion of the Activation Data needed to operate a CA Private Key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA Private Key or the Activation Data to operate a CA Private Key in order to enforce multi-person control over CA Private Key operations under Section 6.2 of the CP and CPS
Secure Sockets Layer (SSL)	The industry-standard (now depreciated, replaced by TLS) method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity,

	and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Session Key	A Symmetric Cryptography Key generated specifically for use within a single transaction or session.
Subject	The holder of a Private Key corresponding to a Public Key. The term "Subject" can, in the case of an organisational Certificate, refer to the equipment or device that holds a Private Key. A Subject is assigned an unambiguous name, which is bound to the Public Key contained in the Subject's Certificate.
Subordinate CA	In a hierarchical PKI, a CA whose Certificate signature Key is certified by another CA, and whose activities are constrained by that other CA. (see Superior CA).
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organisational Certificate, an organisation that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorised to use, the Private Key that corresponds to the Public Key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organisation acts as a Subscriber.
Superior CA	In a hierarchical PKI, a CA who has certified the Certificate signature Key of another CA, and who constrains the activities of that CA. (see Subordinate CA).
Symmetric Cryptography	A class of cryptography in which a single Key is used to both encrypt and decrypt a message. It has two main disadvantages: • for n users, approximately n2 Keys are required; and • confidentiality must be ensured when distributing Keys. (See Asymmetric Cryptography).
System Administrator	An individual who maintains the CA's or RA's hardware and software.
Token	Media capable of storing the Private Key of a Subscriber. Tokens include secure tokens and other devices such as smart cards.
Transport Layer Security (TLS)	The replacement for Secure Sockets Layer (SSL), it is a cryptographic protocol designed to provide secure communications over a network.
Trusted Person	An employee, contractor, or consultant of an entity within the NBN Co PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP.
Trusted Position	The positions within an NBN Co PKI entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognised in classified government nomenclature.

User (Certificate)	(Certificate purpose) A person.
Valid Certificate	A Certificate issued by a CA and accepted by the Subscriber listed in it that has not been revoked or suspended and remains operational.
X.509	The International Telegraph and Telephone Consultative Committee (CCITT1) recommendation X.509 "Information technology - Open Systems Interconnection - The directory: Authentication framework" was published in 1988 to authenticate access to modify parts of the X.500 directory. The Certificates used the X.208 "Abstract Syntax Notation One (ASN.1)" according to a unique subset of the X.209 "Basic Encoding Rules (BER)", called the "Distinguished Encoding Rules (DER)".
X.509 Certificate	Binds an entity's identity, such as a person's name, an asset number, or a position title, to a cryptographic Public Key. The entity (person, asset, or role) is the "subject" or "subscriber" of the Certificate. The identity (name, number, or title) forms the X.500 Distinguished Name (DN) of the Certificate. The Certificate is evidence that the Certification Authority (CA) has verified that the cryptographic Public Key in the Certificate belongs to the entity identified by the DN of the Certificate.

A.1 Acronyms and Abbreviations

AAL	Authentication Assurance Level
ANSI	The American National Standards Institute
AO	Authorising Officer
ASN.1	Abstract Syntax Notation
CA	Certification Authority
CAM	Certification Authority Manager
CAO	Certification Authority Owner
CC	Common Criteria
CO	Certifying Officer
CP	Certificate Policy
CPS	Certification Practice Statement

CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
DN	Distinguished Name
ECC	Elliptic-curve cryptography
EOI	Evidence Of Identity
FIPS	United States Federal Information Processing Standards
HSM	Hardware Security Module
IETF	The Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PIN	Personal Identification number
PKCS	Public-Key Cryptography Standard
PKIX	IETF “Public-Key Infrastructure (X.509)” Working Group standards
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request for comment
RO	Registration Officer
RSA	A Public Key cryptographic system invented by Rivest, Shamir, and Adelman.

S/MIME	Secure multipurpose Internet mail extensions
SAN	Subject Alternate Names
SSL	Secure Sockets Layer
TLS	Transport Layer Security

Appendix B Certificate and CRL Profiles and Formats

B.1 Certificate Profiles and Formats

B.1.1 Certificate Authority Certificates

1. If Certification Authority certificates are issued under the NBN Co Root CA, the following CA certificate format will apply:

Field	Critical	Mandatory	Root Certificate Value	Notes
x.509v1 Fields				
Version		Yes	V3 (2)	Version 3 of X.509
Serial Number		Yes	<octet string>	Must be unique within nbn namespace
Signature algorithm		Yes	<signature_algorithm>	SHA256RSA preferred
Signature hash algorithm		Yes	<signature_hash_algorithm>	SHA256 preferred
Issuer				
Country (C)		Yes	AU	
Organisation (O)		Yes	NBN Co Limited	
Organisational Unit (OU)		No	<CAO_alt>	Optional
Common Name (CN)		Yes	<CA_name>	
Validity				
Not Before		Yes	<datetime>	
Not After		Yes	<datetime>	Maximum date from issue cannot be longer than specified in section 6.3.2
Subject				
Country (C)		Yes	AU	
Organisation (O)		Yes	NBN Co Limited	
Organisational Unit (OU)		No	<CAO_alt>	Optional
Common Name (CN)		Yes	<CA_name>	
Subject Public Key Info		Yes	<subject_public_key>	Public Key encoded in accordance with RFC 3279 & PKCS#1. Key length no less than <Subject_keysize> bits as per Section 6.1.4.

Field	Critical	Mandatory	Root Certificate Value	Notes
x.509v2 Extensions				
issuerUniqueId		No		Shall not be used
SubjectUniqueId		No		Shall not be used
x.509v3 Extensions				
Authority Key Identifier (2.5.29.35)				
Key Identifier	No	Yes	<octet string>	Method hash of the Issuer's Public Key.
AuthorityCertIssuer	No	Yes	Not Present	
AuthorityCertSerialNumber	No	Yes	Not Present	
Subject Key Identifier (2.5.29.15)				
Key Identifier	No	Yes	<octet string>	Method hash of the Issuer's Public Key.
Key Usage (2.5.29.15)				
Digital Signature	Yes	Yes	Set	
Non-Repudiation	Yes	Yes	Not Set	
Key Encipherment	Yes	Yes	Not Set	
Data Encipherment	Yes	Yes	Not Set	
Key Agreement	Yes	Yes	Not Set	
Certificate Signing	Yes	Yes	Set	
CRL Signing	Yes	Yes	Set	
(KEX) Encipher Only	Yes	Yes	Not Set	
(KEX) Decipher Only	Yes	Yes	Not Set	
Certificate Policies				
Policy Identifier 1				
Policy Identifier	No	Yes	<subject_CA_policy_OID>	
CPS Pointer	No	Yes	https://pki.nbnco.net.au/CPS	
User Notice	No	Yes	1.3.6.1.5.5.7.2.2	
Explicit Text	No	Yes	Issued under NBN Co PKI. Refer to https://pki.nbnco.net.au for more information	
Policy Identifier 2				

Field	Critical	Mandatory	Root Certificate Value	Notes
Policy Identifier	No	Yes	<OID>	
User Notice	No	Yes	1.3.6.1.5.5.7.2.2	
Explicit Text	No	Yes	Certificates issued for NBN Co Private <NBN Co Environment> Use	
Basic Constraints				
Subject Type	Yes	Yes	Certificate Authority	
Path Length Constraint	Yes	Yes	Not Set (for NBN Co Root & Intermediate CA's) Set to 0 (for NBN Co Issuing CA's)	
CRL Distribution Points				
Distribution Point	No	Yes	http://crl.nbnco.net.au/CA/	
Reasons	No	Yes	Not Present	
CRL Issuer	No	Yes	Not Present	
Authority Information Access (1.3.6.1.5.5.7.1.1)				
Access Method	No	No	1.3.6.1.5.5.7.48.2	
Access Location	No	No	https://pki.nbnco.net.au/<Ca_location>	

B.1.2 End Entity Certificates

1. If End Entity (User or Device) certificates are issued under an NBN Co Root CA chain, the following certificate format will apply:

Field	Critical	Mandatory	Certificate Value	Notes
x.509v1 Fields				
Version		Yes	V3 (2)	Version 3 of X.509
Serial Number		Yes	<octet string>	Must be unique within nbn namespace
Signature Algorithm		Yes	<signature_algorithm>	SHA256RSA preferred
Signature hash algorithm		Yes	<signature_hash_algorithm>	SHA256 preferred
Issuer				
Country (C)		Yes	AU	

Field	Critical	Mandatory	Certificate Value	Notes
Organisation (O)		Yes	NBN Co Limited	
Organisational Unit (OU)		No		Optional
Common Name (CN)		Yes	<entity_name>	
Validity				
Not Before		Yes	<datetime>	
Not After		Yes	<datetime>	Maximum date from issue cannot be longer than specified in section 6.3.2
Subject				
Country (C)		Yes	AU	
Organisation (O)		Yes	NBN Co Limited	
Organisational Unit (OU)		No		
Common Name (CN)		Yes	<entity_name >	
Subject Public Key Info		Yes	<subject_public_key>	Public Key encoded in accordance with RFC 3279 & PKCS#1. Key length no less than <Subject_keysize> bits as per Section 6.1.4.
x.509v2 Extensions				
issuerUniqueId		No		Shall not be used
SubjectUniqueId		No		Shall not be used
x.509v3 Extensions				
Authority Key Identifier (2.5.29.35)				
Key Identifier	No	Yes	<octet string>	Method hash of the Issuer's Public Key.
AuthorityCertIssuer	No	Yes	Not Present	
AuthorityCertSerialNumber	No	Yes	Not Present	
Subject Key Identifier (2.5.29.15)				
Key Identifier	No	Yes	<octet string>	Method hash of the Issuer's Public Key.
Key Usage (2.5.29.15)				
Digital Signature	Yes	Yes	As Required	Set as required by Section 6.1.6 & Section 7 of this CP document

Field	Critical	Mandatory	Certificate Value	Notes
Non-Repudiation	Yes	Yes	As Required	Set as required by Section 6.1.6 & Section 7 of this CP document
Key Encipherment	Yes	Yes	As Required	Set as required by Section 6.1.6 & Section 7 of this CP document
Data Encipherment	Yes	Yes	As Required	Set as required by Section 6.1.6 & Section 7 of this CP document
Key Agreement	Yes	Yes	As Required	Set as required by Section 6.1.6 & Section 7 of this CP document
Certificate Signing	Yes	Yes	Not Set	
CRL Signing	Yes	Yes	Not Set	
(KEX) Encipher Only	Yes	Yes	Not Set	
(KEX) Decipher Only	Yes	Yes	Not Set	
Certificate Policies				
Policy Identifier 1				
Policy Identifier	No	Yes	<subject_CA_policy_OID>	
CPS Pointer	No	Yes	https://pki.nbnco.net.au/CPS	
User Notice	No	Yes	1.3.6.1.5.5.7.2.2	
Explicit Text	No	Yes	Issued under NBN Co PKI. Refer to https://pki.nbnco.net.au for more information	
Policy Identifier 2				
Policy Identifier	No	Yes	<OID>	
User Notice	No	Yes	1.3.6.1.5.5.7.2.2	
Explicit Text	No	Yes	Certificates issued for NBN Co Private <NBN Co Environment> Use	
Basic Constraints				
Subject Type	Yes	Yes	End Entity	
CRL Distribution Points				

Field	Critical	Mandatory	Certificate Value	Notes
Distribution Point	No	Yes	http://crl.one.au.digicert.com/<CA-Name>.crl	
Reasons	No	Yes	Not Present	
CRL Issuer	No	Yes	Not Present	
Authority Information Access (1.3.6.1.5.5.7.1.1)				
Access Method	No	No	1.3.6.1.5.5.7.48.2	
Access Location	No	No	http://ocsp.one.au.digicert.com	

B.2 CRL Profiles and Formats

1. CRLs issued under an NBN Co Basic, Medium, or High Assurance CA will contain the following CRL format:

Field	Critical	Mandatory	CRL Value	Notes
x.509v1 CRL Fields				
Version		Yes	V2 (1)	Version 2 of X.509 CRL
Signature Algorithm		Yes	<signature_algorithm>	
Issuer				
Country (C)		Yes	AU	
Organisation (O)		Yes	NBN Co Limited	
Organisation Unit (OU)		No	<CAO_alt>	
Common Name (CN)		Yes	<CA_name>	
Validity				
This Update		Yes	<datetime>	
Next Update		Yes	<datetime>	
Revoked Certificates				
Revoked Certificates		Yes	<serial_number>	The revoked certificate serial numbers.
x.509v2 CRL Extensions				

Field	Critical	Mandatory	CRL Value	Notes
Authority Key Identifier (2.5.29.35)				
Key Identifier	No	Yes	<octet string>	Method hash of the Issuer's Public Key.
AuthorityCertIssuer	No	Yes	Not Present	
AuthorityCertSerialNumber	No	Yes	Not Present	
CRL Number (2.5.29.20)	No	Yes	<integer>	Unique positive non-zero integer assigned by the issuing CA