nbn Public Key Infrastructure - Certification Practice Statement

Document Owner	**nbn** PKIPA
Status	Final
Issue date	3 NOV. 22
Revision number	2.2

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.

Contents

1. Introduction 10

1.1 Overview 10

1.2 Document Name and Identification 11

1.2.1 Policy Object Identification 11

1.2.2 Related documents 11

1.3 PKI Participants 11

1.3.1 Certification Authority Owner 11

1.3.2 Policy Authority 11

1.3.3 Certification Authorities 12

1.3.4 Registration Authorities 12

1.3.5 Subscribers 12

1.3.6 Relying Parties 12

1.3.7 Other Participants 12

1.4 Certificate Usage 12

1.4.1 Appropriate Certificate Uses 12

1.4.2 Prohibited Certificate Uses 12

1.5 Policy Administration 13

1.5.1 Organisation Administering the Document 13

1.5.2 Contact Person 13

1.5.3 Person Determining CPS Suitability for the Policy 13

1.5.4 CPS Approval Procedures 13

1.6 Definitions and Acronyms 13

2. Publication and Repository Responsibilities 13

2.1 Repositories 13

2.2 Publication of Certificate Information 13

2.3 Time or Frequency of Publication 14

2.4 Access Controls on Repositories 14

3. Identification and Authentication 14

3.1 Naming 14

3.1.1 Types of Names 14

3.1.2 Need for Names to be Meaningful 14

3.1.3 Anonymity or Pseudonymity of Subscribers 14
3.1.4 Rules for Interpreting Various Name Forms 14
3.1.5 Uniqueness of Names 14
3.1.6 Recognition, Authentication, and Role of Trademarks 14
3.2 Initial Identity Validation 14
3.2.1 Method to Prove Possession of Private Key 14
3.2.2 Authentication of Organisation Identity 15
3.2.3 Authentication of Individual Identity 15
3.2.4 Non-verified Subscriber Information 15
3.2.5 Criteria for Interoperation 15
3.3 Identification and Authentication for Re-key Requests 15
3.4 Identification and Authentication for Revocation Requests 15
4. Certificate Life-Cycle Operational Requirements 16
4.1 Certificate Application 16
4.1.1 Who Can Submit a Certificate Application 16
4.1.2 Enrolment Process and Responsibilities 16
4.2 Certificate Application Processing 17
4.2.1 Performing Identification and Authentication Functions 17
4.2.2 Approval or Rejection of Certificate Applications 17
4.2.3 Time to Process Certificate Applications 17
4.3 Certificate Issuance 17
4.3.1 CA Actions during Certificate Issuance 17
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 17
4.4 Certificate Acceptance 17
4.4.1 Conduct Constituting Certificate Acceptance 17
4.4.2 Publication of the Certificate by the CA 17
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 17
4.5 Key Pair and Certificate Usage 18
4.5.1 Subscriber Private Key and Certificate Usage 18
4.5.2 Relying Party Public Key and Certificate Usage 18
4.6 Certificate Renewal 18
4.6.1 Circumstance for Certificate Renewal 18
4.6.2 Who May Request Renewal 18

4.6.3 Processing Certificate Renewal Requests 18
4.6.4 Notification of New Certificate Issuance to Subscriber 18
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 18
4.6.6 Publication of the Renewal Certificate by the CA 19
4.6.7 Notification of Certificate Issuance by the CA to other Entities 19
4.7 Certificate Re-key 19
4.7.1 Circumstance for Certificate Re-key 19
4.7.2 Who May Request Certification of a New Public Key 19
4.7.3 Processing Certificate Re-keying Requests 19
4.7.4 Notification of New Certificate Issuance to Subscriber 19
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 19
4.7.6 Publication of the Re-keyed Certificate by the CA 19
4.7.7 Notification of Certificate Issuance by the CA to other Entities 19
4.8 Certificate Modification 20
4.8.1 Circumstance for Certificate Modification 20
4.8.2 Who May Request Certificate Modification 20
4.8.3 Processing Certificate Modification Requests 20
4.8.4 Notification of New Certificate Issuance to Subscriber 20
4.8.5 Conduct Constituting Acceptance of a Modified Certificate 20
4.8.6 Publication of the Modified Certificate by the CA 20
4.8.7 Notification of Certificate Issuance by the CA to other Entities 20
4.9 Certificate Revocation and Suspension 20
4.9.1 Circumstances for Revocation 20
4.9.2 Who Can Request Revocation 21
4.9.3 Procedure for Revocation Requests 21
4.9.4 Revocation Request Grace Period 22
4.9.5 Time within which CA must Process the Revocation Request 22
4.9.6 Revocation Checking Requirement for Relying Parties 22
4.9.7 CRL Issuance Frequency 22
4.9.8 Maximum Latency for CRLs 22
4.9.9 On-Line Revocation/Status Checking Availability 22
4.9.10 On-Line Revocation Checking Requirements 22
4.9.11 Other Forms of Revocation Advertisements Available 22

4.9.12 Special Requirements Related to Key Compromise 22
4.9.13 Circumstances for Suspension 22
4.9.14 Who Can Request Suspension 22
4.9.15 Procedure for Suspension Request 22
4.9.16 Limits on Suspension Period 23
4.10 Certificate Status Services 23
4.11 End of Subscription 23
4.12 Key Escrow and Recovery 23
4.12.1 Key Escrow and Recovery Policy and Practices 23
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 23
5. Facility, Management, and Operational Controls 24
5.1 Physical Controls 24
5.1.1 Site Location and Construction 24
5.1.2 Physical Access 24
5.1.3 Power and Air Conditioning 24
5.1.4 Water Exposures 24
5.1.5 Fire Prevention and Protection 24
5.1.6 Media Storage 25
5.1.7 Waste Disposal 25
5.1.8 Off-Site Backup 25
5.2 Procedural Controls 25
5.2.1 Trusted Roles 25
5.2.2 Number of Persons Required for Task 25
5.2.3 Identification and Authentication for Each Role 26
5.2.4 Roles Requiring Separation of Duties 26
5.3 Personnel Security Controls 26
5.3.1 Qualifications, Experience, and Clearance Requirements 26
5.3.2 Background Check Procedures 27
5.3.3 Training Requirements 27
5.3.4 Retraining Frequency and Requirements 27
5.3.5 Job Rotation Frequency and Sequence 27
5.3.6 Sanctions for Unauthorised Actions 28
5.3.7 Independent Contractor Requirements 28

5.3.8 Documentation Supplied to Personnel 28
5.4 Audit Logging Procedures 28
5.4.1 Types of Events Recorded 28
5.4.2 Frequency of Processing Log 29
5.4.3 Retention Period of Audit Log 29
5.4.4 Protection of Audit Log 29
5.4.5 Audit Log Backup Procedures 29
5.4.6 Audit Collection System (Internal vs. External) 29
5.4.7 Notification to Event-Causing Subject 29
5.4.8 Vulnerability Assessments 29
5.5 Records Archival 29
5.5.1 Types of Records Archived 29
5.5.2 Retention Period of Archive 29
5.5.3 Protection of Archive 30
5.5.4 Archive Backup Procedures 30
5.5.5 Requirements for Timestamping of Records 30
5.5.6 Archive Collection System (Internal vs. External) 30
5.5.7 Procedures to Obtain and Verify Archive Information 30
5.6 Key Changeover 30
5.7 Compromise and Disaster Recovery 31
5.7.1 Incident and Compromise Handling Procedures 31
5.7.2 Computing Resources, Software, and/or Data are corrupted 31
5.7.3 Entity Private Key Compromise Procedures 31
5.7.4 Business Continuity Capabilities after a Disaster 31
5.8 CA or RA Termination 32
6. Technical Security Controls 32
6.1 Key Pair Generation and Installation 32
6.1.1 Key Pair Generation 32
6.1.2 Private Key Delivery to Subscriber 33
6.1.3 Public Key Delivery to Certificate Issuer 33
6.1.4 Key Sizes 33
6.1.5 Public Key Parameters Generation and Quality Checking 33
6.1.6 Key Usage Purposes (as per X.509 V3 Key Usage Field) 33

6.2 Private Key Protection and Cryptographic Module Engineering Controls 33
6.2.1 Cryptographic Module Standards and Controls 33
6.2.2 Private Key (m out of n) Multi-Person Control 34
6.2.3 Private Key Escrow 34
6.2.4 Private Key Backup 34
6.2.5 Private Key Archival 34
6.2.6 Private Key Transfer into or From a Cryptographic Module 34
6.2.7 Private Key Storage on Cryptographic Module 34
6.2.8 Method of Activating Private Key 35
6.2.9 Method of Deactivating Private Key 36
6.2.10 Method of Destroying Private Key 36
6.2.11 Cryptographic Module Rating 36
6.3 Other Aspects of Key Pair Management 36
6.3.1 Public Key Archival 36
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 36
6.4 Activation Data 36
6.4.1 Activation Data Generation and Installation 36
6.4.2 Activation Data Protection 36
6.4.3 Other Aspects of Activation Data 37
6.5 Computer Security Controls 37
6.5.1 Specific Computer Security Technical Requirements 37
6.5.2 Computer Security Rating 37
6.6 Life Cycle Security Controls 37
6.6.1 System Development Controls 37
6.6.2 Security Management Controls 38
6.6.3 Life Cycle Security Controls 38
6.7 Network Security Controls 38
6.8 Timestamping 38
7. Certificate, CRL, and OCSP Profiles 38
7.1 Certificate Profile 38
7.2 CRL Profiles 38
7.3 OCSP Profiles 38

8. Compliance Audit and Other Assessments 39

8.1 Frequency or Circumstances of Assessment 39

8.2 Identity/Qualifications of Assessor 39

8.3 Assessor's Relationship to Assessed Entity 39

8.4 Topics Covered by Assessment 39

8.5 Actions Taken as a Result of Deficiency 39

9. Other Business and Legal Matters 39

9.1 Fees 39

9.2 Confidentiality 39

9.3 Privacy 40

9.4 Intellectual Property Rights 40

9.5 Term and Termination 40

9.5.1 Term 40

9.5.2 Termination 40

9.5.3 Effect of Termination and Survival 40

9.6 Individual Notices and Communications with Participants 40

9.7 Amendments 40

9.7.1 Procedure for Amendment 40

9.7.2 Circumstances under Which OID Must Be Changed 41

9.8 Governing Law 41

9.9 Compliance with Applicable Law 41

1. Introduction

In general, a Certification Practice Statement (CPS) is a statement of the practices that a Certification Authority (CA) employs for all certificate lifecycle services (e.g., issuance, management, revocation, and renewal or re-keying) and provides details concerning other business, legal, and technical matters. A Certificate Policy (CP) is a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements.
The headings in this CPS follow the framework set out in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
A document hierarchy applies: the provisions of any applicable contract such as a *Subscriber Agreement*, *Deed of Agreement* or other relevant contract override the provisions of a CP. The provisions of a CP prevail over the provisions of this CPS to the extent of any direct inconsistency. The provisions of this CPS govern any matter on which a CP is silent. (Note: where subtitled sections of the framework provide no additional information to detail provided in a CP they have not been further extrapolated in this document.)
This section identifies and introduces the set of provisions and indicates the types of entities and applications to which this **nbn** x.509 CPS applies.

1.1 Overview

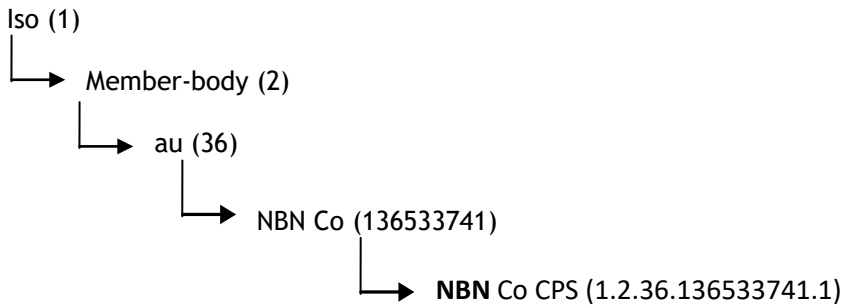
1. This document is the NBN Co Public Key Infrastructure (PKI) Certification Practice Statement (CPS). It states the practices that the Certification Authorities (CA) employ in providing certification services in accordance with the NBN Co Public Key Infrastructure Framework (NBN Co PKI Framework) and the specific requirements of each applicable Certificate Policy (CP).
2. This CPS describes the practices employed by NBN Co to meet the requirements of each applicable CP and the NBN Co Framework.
3. The CPs are the principal statements of policy governing the NBN Co PKI and are given in separate documents. They establish the business, legal, and technical requirements for certification services in accordance with the NBN Co PKI Framework.
4. While each CP sets forth requirements that participants must meet, this CPS describes how NBN Co meets these requirements and describes the practices that NBN Co employs for securely managing the infrastructure that supports the NBN Co PKI CAs, and issuing, renewing, re-keying, or revoking NBN Co issued Certificates in accordance with the requirements of each applicable CP and the NBN Co PKI Framework.
5. This document provides the standard set of provisions to define this CPS and describes the practices followed by a CA under which the binding of the Distinguished Name (DN) and the Public Key of a subject occurs.
6. This CPS is applicable to all NBN Co CAs.
7. Disclosure of the CPS is detailed in the Subscriber and/or Relying Party Agreements.
8. This CPS and any subordinate CPSs, where used, shall be approved by the NBN Co Public Key Infrastructure Policy Authority (NBN Co PKIPA).
9. In some instances, this CPS refers to ancillary confidential security and operational documents for specific detailed practices, where including the specifics in this CPS could compromise the security of the NBN Co PKI.
10. This CPS is a policy document and does not form (and is not intended to form) a legally binding agreement. Contractual obligations will be set out in other agreements such as Subscriber Agreements and Relying Party Agreements.

1.2 Document Name and Identification

1. Document Name: **nbn Public Key Infrastructure - Certification Practice Statement**
2. Document Public Location: https://pki.nbnco.net.au/CPS
3. Document X.500 OID: **1.2.36.136533741.1**

1.2.1 Policy Object Identification

1. The OIDs registered by NBN Co for the Certification Practice Statement policy is shown below. These OIDs are registered under the NBN Co Limited arc as:



1.2.2 Related documents

Table 1 – Related documents

Document		Owner	Availability
[1]	**NBN** Co Limited – Public Key Infrastructure – Certificate Policy	nbn	Public
[2]	**NBN** Co Public Key Infrastructure Framework Overview	nbn	Internal use only
[3]	Subscriber Agreement	DigiCert	Public
[4]	Relaying Party Agreement	DigiCert	Public
[5]	Relaying 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 the purpose of this CPS, the CAO is NBN Co Limited.

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. Certification Authorities (CA) are entities that sign and issue Certificates. CAs may register Subscribers themselves or may delegate that function to one or more separate Registration Authorities (RA).
2. The CAs employing this CPS use trusted roles (Refer to Section 5.2.1).

1.3.4 Registration Authorities

1. Registration Authorities (RA) may be delegated by CAs to perform Identification and registration of Subscribers and associated functions. RAs are not permitted to sign Certificates.
2. The RAs subject to this CPS use trusted roles (Refer to Section 5.2.1).

1.3.5 Subscribers

1. Subscribers of Certificates issued by a CA employing this CPS are entities that contract that CA for the issuance of Certificates.
2. All Subscribers agree to be bound by the terms of the applicable Subscriber Agreement to be issued Certificates.
3. Where a Subscriber delegates responsibility for initiating applications for Certificates to a system, the Subscriber agrees to ensure that the system meets the terms and conditions of the Subscriber Agreement.

1.3.6 Relying Parties

1. Relying Parties rely on the binding of the Public Key to the Distinguished Name (DN) of a subject in a Certificate to the stated level of certification assurance.
2. All Relying Parties agree to be bound by the terms of a Relying Party Agreement. The act of relying on an NBN Co PKI Certificate constitutes acceptance of the applicable Certificate Policy and Relying Party Agreement.

1.3.7 Other Participants

1.3.7.1 Auditors and Assessors

1. Besides the auditor roles and functions of the various authorities, from time-to-time external third-party auditor entities are engaged to verify the compliance provisions of the NBN Co PKI.

1.4 Certificate Usage

1. Refer to the NBN Co PKI Framework, the applicable Certificate Policy, Subscriber Agreement, and Relying Party Agreement.
2. The level of assurance in the certification is in accordance with the NBN Co PKI Framework.

1.4.1 Appropriate Certificate Uses

1. Refer to the NBN Co PKI Framework, the applicable Certificate Policy, and the Subscriber and/or Relying Party Agreements.

1.4.2 Prohibited Certificate Uses

1. Refer to the applicable Certificate Policy and the Subscriber and/or Relying Party Agreements, and the Subscriber and Relying Party Agreements.

2. NBN Co Certificates are not designed, intended, or authorised for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.
3. CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

1. The registration and maintenance of this CPS is the responsibility of the NBN Co PKI Certification Authority Manager (CAM).

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 determines the suitability and applicability of this CPS.

1.5.4 CPS Approval Procedures

1. Approval of this CPS and subsequent amendments shall be made by the NBN Co PKIPA.
2. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be available from the NBN Co PKI Repository located at https://pki.nbnco.net.au/CPS.
3. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

1.6 Definitions and Acronyms

1. All definitions and acronyms are listed in 9.9 Appendix A of this document.

2. Publication and Repository Responsibilities

2.1 Repositories

1. An authoritative repository for all PKI-related information issued by any CA using this CPS is located under the URL https://pki.nbnco.net.au/ and made available to all Subscribers and Relying Parties of those Certificates as detailed in the respective Subscriber and Relying Party Agreements.
2. Certificate revocation lists using this CPS will be hosted in a separate repository located under the URL http://crl.nbnco.net.au/.

2.2 Publication of Certificate Information

1. The Certification Practice Statement, Certificate Policy, CA Certificate, and Certificate status information are available from the repository.

2.3 Time or Frequency of Publication

1. Refer to the appropriate Certificate Policy.

2.4 Access Controls on Repositories

1. Information published in the NBN Co PKI Repository is publicly accessible information. Read only access to such information is unrestricted. NBN Co requires persons to agree to a Relying Party Agreement as a condition of accessing Certificates, Certificate status information, or CRLs.

3. Identification and Authentication

3.1 Naming

1. Names appearing in Certificates are constructed in accordance with the relevant Certificate Policy and the NBN Co PKI Framework.

3.1.1 Types of Names

1. Refer to the Certificate Policy.

3.1.2 Need for Names to be Meaningful

1. Refer to the Certificate Policy.

3.1.3 Anonymity or Pseudonymity of Subscribers

1. Refer to the Certificate Policy.

3.1.4 Rules for Interpreting Various Name Forms

1. Refer to the Certificate Policy.

3.1.5 Uniqueness of Names

1. Refer to the Certificate Policy.

3.1.6 Recognition, Authentication, and Role of Trademarks

1. Certificate applicants are prohibited from using names in their Certificate applications that infringe upon the Intellectual Property Rights of others. NBN Co, however, does not verify whether a Certificate applicant has Intellectual Property Rights in the name appearing in a Certificate application or arbitrates, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. NBN Co is entitled, without liability to any Certificate applicant, to reject or suspend any Certificate application because of such dispute.

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 shall be auditable. Refer to Section 6.1 and 6.2 .

3.2.2 Authentication of Organisation Identity

1. Whenever a CA Certificate is to contain an organisation name, the identity of the organisation and other enrolment information is confirmed in accordance with the NBN Co PKI Framework.
2. For Organisations using NBN Co's MPKI service, NBN Co, as the Issuing CA hosting provider will confirm the following:
    a. Said Organisation exists in a business database (e.g., Dun and Bradstreet), or alternatively, has organisational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organisation;
    b. Conducts business at the address listed in the agreement; and
    c. Confirms with the organisation by telephone, postal mail, or comparable procedure certain information about the organisation, that the organisation has authorised the NBN Co MPKI Service application, and that the person submitting the NBN Co MPKI Service application is authorised to do so.

3.2.3 Authentication of Individual Identity

1. A Registration Officer verifies the identity of the Subscriber in accordance with the NBN Co PKI Framework.

3.2.4 Non-verified Subscriber Information

1. Refer to the Certificate Policy.

3.2.5 Criteria for Interoperation

1. Refer to the Certificate Policy.

3.3 Identification and Authentication for Re-key Requests

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

3.4 Identification and Authentication for Revocation Requests

1. Prior to the revocation of a CA Certificate, NBN Co verifies that the revocation has been requested by an authorised entity.
2. For revocation of end-entity subscriber Certificates issued from an NBN Co MPKI Service, the acceptable procedures for authenticating the revocation requests of a Subscriber include:
    a. Having the Subscriber for certain Certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof) and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record.
    b. The authorised MPKI RA receiving a message from the Subscriber that requests revocation and contains a Digital Signature verifiable with reference to the Certificate to be revoked. In cases

where the private key has been compromised, the said private key cannot be used as subscriber identification.

c. Communication with the Subscriber providing reasonable assurances considering the Assurance Level of Certificate that the person or organisation requesting revocation is in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, email, mail, or courier service.

3. RA's using an Automated Administration Software Module may submit bulk revocation requests. Such requests shall be authenticated via a digitally signed request signed with the Private Key in the RA's Automated Administration hardware token.
4. Any request to revoke a CA Certificate shall be authenticated by NBN Co to ensure that the revocation has in fact been requested by an appropriately authorised party.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

1. Certificate applications are initiated by Subscribers to a Registration Officer (RO).
2. The following may initiate Certificate applications:
   a. Any individual who is the subject of the Certificate.
   b. Any authorised representative of an Organisation or entity.
   c. Any authorised representative of a CA.
   d. Any authorised representative of an RA.
3. The RO provides a signed Certificate request to the Authorising Officer (AO).

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 CA and RA Certificates

1. Subscribers of CA and RA Certificates enter into a contract with the into the relevant Subscriber Agreement with the NBN Co. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process.

4.1.2.2 End-user Certificate Subscribers

1. All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement and undergo an enrolment process consisting of:
   a. Completing a Certificate application and providing true and correct information;
   b. Generating, or arranging to have generated, a key pair;
   c. Delivering his, her, or its Public Key to the RA; and
   d. Demonstrating possession and/or exclusive control of the Private Key corresponding to the Public Key.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

1. The RO shall perform Identification and authentication of all required Subscriber information in terms of Section 3.2

4.2.2 Approval or Rejection of Certificate Applications

1. The RO shall approve an application for a Certificate if:
    a. Successful identification and authentication of all required Subscriber information in terms of Section 3.2 and
    b. Applicable departmental and financial requirements have been met.
2. The RO shall reject a Certificate application if:
    a. Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
    b. The Subscriber fails to furnish supporting documentation upon request, or
    c. The Subscriber fails to respond to notices within a specified time, or
    d. The RA believes that issuing a Certificate to the Subscriber may bring the NBN Co PKI into disrepute.

4.2.3 Time to Process Certificate Applications

1. Refer to the Certificate Policy.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

1. The Certifying Officer (CO) authenticates the approved request from the AO.
2. The CO publishes the Certificate in accordance with Section 4.4.2

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

1. Refer to the Certificate Policy.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

1. Refer to the Certificate Policy.

4.4.2 Publication of the Certificate by the CA

1. Refer to the Certificate Policy.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

1. Refer to the Certificate Policy.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

1. Refer to the Certificate Policy.

4.5.2 Relying Party Public Key and Certificate Usage

1. Refer to the Certificate Policy.

4.6 Certificate Renewal

1. Refer to the Certificate Policy.

4.6.1 Circumstance for Certificate Renewal

1. Refer to the Certificate Policy.

4.6.2 Who May Request Renewal

1. Refer to the Certificate Policy.

4.6.3 Processing Certificate Renewal Requests

1. The person or organisation seeking to renew an end-user Subscriber Certificate shall be authenticated as the Subscriber (or authorised by the Subscriber) of the Certificate by one of the following procedures:
    a. Proof of possession of the Private Key;
    b. Subscribers choose and submit with their enrolment information a Challenge Phrase (or the equivalent thereof); Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's re-enrolment information, and the enrolment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is issued;
    c. For automated certificate renewal, the PKI solution will verify the End-Entity Domain credentials and Domain Group membership permissions;
    d. The RO may send an e-mail message to the e-mail address associated with the verified corporate contact for the Certificate being renewed, requesting confirmation of the Certificate renewal order and authorisation to issue the Certificate; Upon receipt of confirmation authorising issuance of the Certificate, the RO will proceed if the enrolment information (including Corporate and Technical contact information) has not changed.
2. Other than these procedures or another PA-approved procedure, the requirements for the authentication of an original Certificate application shall be used for renewing an end-user Subscriber Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

1. Refer to the Certificate Policy.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

1. Refer to the Certificate Policy.

4.6.6 Publication of the Renewal Certificate by the CA

1. Refer to the Certificate Policy.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

1. Refer to the Certificate Policy.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

1. Refer to the Certificate Policy.

4.7.2 Who May Request Certification of a New Public Key

1. Refer to the Certificate Policy.

4.7.3 Processing Certificate Re-keying Requests

1. The person or organisation seeking to re-key an end-user Subscriber Certificate shall be authenticated as the Subscriber (or authorised by the Subscriber) of the Certificate by one of the following procedures:
    a. Proof of possession of the Private Key;
    b. Subscribers choose and submit with their enrolment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's re-enrolment information, and the enrolment information (including contact information) has not changed, a renewal Certificate is issued.
    c. For automated certificate renewal, the PKI solution will verify the End-Entity Domain credentials and Domain Group membership permissions.
2. Other than this procedure or another PA-approved procedure, the requirements for the authentication of an original Certificate application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

1. Refer to the Certificate Policy.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

1. Refer to the Certificate Policy.

4.7.6 Publication of the Re-keyed Certificate by the CA

1. Refer to the Certificate Policy.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

1. Refer to the Certificate Policy.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

1. Refer to the Certificate Policy.
2. A modified Certificate is required to maintain the same level of trust and assurance as the original issued certificate.

4.8.2 Who May Request Certificate Modification

1. Refer to the Certificate Policy.

4.8.3 Processing Certificate Modification Requests

1. Refer to the Certificate Policy.

4.8.4 Notification of New Certificate Issuance to Subscriber

1. Refer to the Certificate Policy.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

1. Refer to the Certificate Policy.

4.8.6 Publication of the Modified Certificate by the CA

1. Refer to the Certificate Policy.

4.8.7 Notification of Certificate Issuance by the CA to other Entities

1. Refer to the Certificate Policy.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

1. In the circumstances listed below an end-user Subscriber Certificate will be revoked by the NBN Co (or by the Subscriber) and published on a CRL.
2. An end-user Subscriber Certificate may be revoked by NBN Co (in its sole and exclusive discretion) if:
    a. The NBN Co or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's Private Key.
    b. The NBN Co has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement.
    c. The Subscriber Agreement with the Subscriber has been terminated.
    d. The affiliation between the NBN Co and a Subscriber is terminated or has otherwise ended.
    e. The affiliation between an entity that is a Subscriber of a Device, User, or Organisation Certificate and the organisational representative controlling the Subscriber's Private Key is terminated or has otherwise ended.
    f. The NBN Co has reason to believe that:
        i. the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CP,

ii. the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or
iii. the Certificate was issued without the authorisation of the entity named as the Subject of such Certificate.

g. The NBN Co has reason to believe that a material fact in the Certificate application is false.
h. The NBN Co determines that a material prerequisite to Certificate issuance was neither satisfied nor waived.
i. In the case of High Assurance Certificates, the Subscriber's organisation name changes.
j. The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has changed.
k. The NBN Co has reason to believe that the Certificate was obtained by way of fraud, deception, or other equivalent means.
l. The NBN Co considers that the continued use of that Certificate is harmful or otherwise detrimental to the NBN Co PKI, in which case, the NBN Co may consider, among other things, the following:
i. The nature and number of complaints or claims received.
ii. The identity of the complainant(s) or claimant(s).
iii. Relevant legislation in force.
iv. Responses to the alleged harmful use from the Subscriber.
v. Any other relevant matters.

3. NBN Co Subscriber Agreements require each end-user Subscriber to immediately notify NBN Co of a known or suspected compromise of its Private Key.

4.9.2 Who Can Request Revocation

1. Individual Subscribers can request the revocation of their own individual Certificates. In the case of Device and Organisation Certificates, a duly authorised representative of the Subscriber shall be entitled to request the revocation of Certificates issued to the Subscriber. A duly authorised representative of the NBN Co or an RO shall be entitled to request the revocation of an RO Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.
2. Only NBN Co is entitled to request or initiate the revocation of the Certificates issued to its own CAs. RAs are entitled, through their duly authorised representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.9.3 Procedure for Revocation Requests

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

1. An end-user Subscriber requesting revocation is required to communicate the request to the RO, who in turn will initiate revocation of the Certificate promptly. Communication of such revocation request shall be in accordance with Section 3.4
2. Should the CA or RA require a Subscriber certificate revoked; The CA or RA must inform the Subscriber of the pending revocation with a written notice and reasoning prior any revocation. Opportunity will be given for the Subscriber to dispute the revocation, however if requested by the CA this cannot be overruled.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

1. A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to the appropriate PA. The PA will then initiate revocation of the Certificate. The NBN Co PKIPA may also initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

1. Revocation requests shall be submitted as promptly as possible within a reasonable time of becoming aware of a revocation circumstance.

4.9.5 Time within which CA must Process the Revocation Request

1. NBN Co takes reasonable steps to process revocation requests as soon as reasonably possible.

4.9.6 Revocation Checking Requirement for Relying Parties

1. Refer to the Certificate Policy.

4.9.7 CRL Issuance Frequency

1. CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least annually, but also whenever a CA Certificate is revoked.
2. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.9.8 Maximum Latency for CRLs

1. The NBN Co hosted CA CRLs are posted to the repository within a reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability

1. Refer to the Certificate Policy.

4.9.10 On-Line Revocation Checking Requirements

1. Refer to the Certificate Policy.

4.9.11 Other Forms of Revocation Advertisements Available

1. Refer to the Certificate Policy.

4.9.12 Special Requirements Related to Key Compromise

1. The NBN Co uses reasonable efforts to notify potential Relying Parties if it discovers, or has reason to believe, that there has been a compromise of the Private Key of one of its hosted CAs.

4.9.13 Circumstances for Suspension

1. Refer to the Certificate Policy.

4.9.14 Who Can Request Suspension

1. Refer to the Certificate Policy.

4.9.15 Procedure for Suspension Request

1. Refer to the Certificate Policy.

4.9.16 Limits on Suspension Period

1. Refer to the Certificate Policy.

4.10 Certificate Status Services

1. Refer to the Certificate Policy.

4.11 End of Subscription

1. A Subscriber may end a subscription for an NBN Co Certificate by:
    a. Allowing the Certificate to expire without renewing or re-keying that Certificate, or
    b. Revoking the Certificate before Certificate expiration without replacing the Certificate.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

1. Escrowed Private Keys shall be stored in encrypted form using the Managed PKI Key Manager software.
2. End-user Subscriber Private Keys shall only be recovered under the circumstances permitted within the Certificate Policy, under which:
    a. CAs using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's Private Key is, in fact, from the Subscriber and not an impostor,
    b. CAs shall recover a Subscriber's Private Key without the Subscriber's authority only for legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and
    c. Such CAs shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorised access to Private Keys.
3. The subject of the key shall be notified should key escrow be requested for their Key, unless specifically forbidden by a court order.
4. It is recommended that CAs using the Managed PKI Key Management Service:
    a. Notify the Subscribers that their Private Keys are escrowed.
    b. Protect Subscribers' escrowed Keys from unauthorised disclosure.
    c. Protect all information, including the administrator's own Key(s) that could be used to recover Subscribers' escrowed Keys.
    d. Release Subscribers' escrowed Keys only for properly authenticated and authorised requests for recovery.
    e. Unless specifically covered by a court order, the certificate should be revoked with the status 'key compromise' in such cases as the key has been accessed by a third party.
    f. Not be required to communicate any information concerning a Key recovery to the Subscriber except when the Subscriber him/herself has requested recovery.
    g. Not disclose or allow to be disclosed escrowed Keys or escrowed Key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organisation policy; or by order of a court of competent jurisdiction.
5. Requests for key escrow should be addressed to the **nbn** co PKIPA.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

1. This information is not publicly available. Relevant parties should contact their PA for more information.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

1. NBN Co has implemented a set of Information Security Policies and Standards which support the security requirements of this CPS. Compliance with these policies and standards is included in
    a. NBN Co's independent Audit requirements described in Section 8. An overview of the requirements is given below.

5.1.1 Site Location and Construction

1. NBN Co CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of sensitive information and systems whether covert or overt.
2. NBN Co also maintains disaster recovery facilities for its CA operations. The NBN Co disaster recovery facilities are protected by multiple tiers of physical security comparable to those of the primary facility used by NBN Co.

5.1.2 Physical Access

1. CA systems used in relation to the NBN Co PKI are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier.
2. Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity—any activity related to the lifecycle of the certification process such as authentication, verification, and issuance—occurs within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged, and video recorded. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.
3. The physical security system includes additional tiers for Key management security, which serves to protect both online and offline storage of CA cryptographic hardware (cryptographic signing units or CSU) and keying material. Online CSUs are protected using locked cabinets. Offline CSUs are protected using locked safes, cabinets, and containers. Access to CSUs and Keying material is restricted in accordance with no less than the NBN Co PKI Framework requirements. The opening and closing of cabinets or containers in these tiers are logged for Audit purposes.

5.1.3 Power and Air Conditioning

1. The NBN Co secure facilities are equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power, and heating/ventilation/air-conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

1. NBN Co has taken reasonable precautions to minimise the impact of water exposure to NBN Co systems.

5.1.5 Fire Prevention and Protection

1. NBN Co has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. The NBN Co fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

1. All media containing production software and data, audit, archive, or backup information is stored within NBN Co facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

1. Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroed in accordance with the manufacturers' guidance prior to disposal.

5.1.8 Off-Site Backup

1. NBN Co performs routine backups of critical system data, Audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded third-party storage facility and the NBN Co disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

1. Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:
    a. The validation of information in Certificate applications.
    b. The acceptance, rejection, or other processing of Certificate applications, revocation requests, renewal requests, or enrolment information.
    c. The issuance or revocation of Certificates, including personnel having access to restricted portions of its repository.
    d. The handling of Subscriber information or requests.
2. Trusted Persons include, but are not limited to:
    a. Customer service personnel.
    b. Cryptographic business operations personnel.
    c. Security personnel.
    d. System administration personnel.
    e. Designated engineering personnel.
    f. Executives that are designated to manage infrastructural trustworthiness.
3. NBN Co considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required for Task

1. NBN Co has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.
2. Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated Key material, require multiple Trusted Persons.
3. These internal control procedures are designed to ensure that at a minimum, two Trusted Persons are required to have either physical or logical access to the device. Access to CA cryptographic hardware is

strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational Keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold —Secret Shares and vice versa.

5.2.3 Identification and Authentication for Each Role

1. For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing NBN Co HR or security functions and a check of well-recognised forms of Identification (e.g., passports and driver's licences). Identity is further confirmed through the background checking procedures in Section 5.3.2
2. NBN Co ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:
    a. Issued access devices and granted access to the required facilities; or
    b. Issued electronic credentials to access and perform specific functions on NBN Co CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

1. Roles requiring Separation of duties include but are not limited to:
    a. The validation of information in Certificate applications;
    b. The acceptance, rejection, or other processing of Certificate applications, revocation requests, renewal requests, or enrolment information;
    c. The issuance or revocation of Certificates, including personnel having access to restricted portions of the repository;
    d. The handling of Subscriber information or requests;
    e. The generation, issuing or destruction of a CA Certificate, and;
    f. The loading of a CA on production.
2. A single individual may request and hold multiple duties; however, this shouldn't conflict with the roles that require specific separation of duties as given in above in paragraph 1.
3. If it is deemed necessary to give a single individual access to multiple roles, then:
    a. All activity by the individual shall be independently reviewed in a timely fashion;
    b. Access shall be limited to completing a specific set of tasks, and;
    c. The additional access shall be removed post completion.

5.3 Personnel Security Controls

1. Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.1 Qualifications, Experience, and Clearance Requirements

1. NBN Co requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

1. Prior to commencement of employment in a Trusted Role, NBN Co conducts background checks which include the following:
    a. Confirmation of previous employment.
    b. Check of professional reference.
    c. Confirmation of the highest or most relevant educational degree obtained.
    d. Search of criminal records (state and national).
    e. Check of credit/financial/insolvency records.
2. To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, NBN Co will utilise a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.
3. The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:
    a. Misrepresentations made by the candidate or Trusted Person.
    b. Highly unfavourable or unreliable professional references.
    c. Certain criminal convictions.
    d. Breach of NBN Co Limited Code of Conduct.
4. Reports containing such information are evaluated by human resources and security personnel, who then determine the appropriate course of action considering the type, magnitude, and frequency of the behaviour uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.
5. The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

1. NBN Co provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. NBN Co maintains records of such training. NBN Co periodically reviews and enhances its training programs as necessary.
2. NBN Co training programs are tailored to the individual's responsibilities and include the following as relevant:
    a. Basic PKI concepts.
    b. Job responsibilities.
    c. NBN Co security and operational policies and procedures.
    d. Use and operation of deployed hardware and software.
    e. Incident and Compromise reporting and handling.
    f. Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

1. NBN Co provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

1. No stipulation.

5.3.6 Sanctions for Unauthorised Actions

1. Appropriate disciplinary actions are taken for unauthorised actions or other violations of NBN Co policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorised actions.

5.3.7 Independent Contractor Requirements

1. In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to an NBN Co employee in a comparable position.
2. Independent contractors and consultants who have not completed or passed the background check procedures specified in Section 5.3.2 are permitted access to NBN Co secure facilities only to the extent they are always escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

1. NBN Co provides its employees with the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

1. NBN Co logs the following significant events:
    a. CA Key life cycle management events, including:
        i. Key generation, backup, storage, recovery, archival, and destruction.
        ii. Cryptographic device life cycle management events.
    b. CA and Subscriber Certificate life cycle management events, including:
        i. Certificate applications, renewal, re-key, and revocation.
        ii. Successful or unsuccessful processing of requests.
        iii. Generation and issuance of Certificates and publishing of CRLs.
        iv. Key escrow activity.
    c. Security-related events including:
        i. Operating system events.
        ii. CA Application events.
        iii. Successful and unsuccessful PKI system access attempts.
        iv. PKI and security system actions performed by NBN Co personnel.
        v. Security sensitive files or records read, written, or deleted.
        vi. Security profile changes.
        vii. System crashes, hardware failures and other anomalies.
        viii. Network device activity.
        ix. CA facility visitor entry/exit.
2. Log entries include the following elements:
    a. Date and time of the entry.
    b. Serial or sequence number of entries, for automatic journal entries.
    c. Identity of the entity making the journal entry.
    d. Type of entry.

5.4.2 Frequency of Processing Log

1. NBN Co reviews its Audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within NBN Co CA systems.

5.4.3 Retention Period of Audit Log

1. Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2

5.4.4 Protection of Audit Log

1. Audit logs are protected with an electronic Audit log system that includes mechanisms to protect the log files from unauthorised viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

1. Full backups of Audit logs are created daily six days per week. (Monday-Saturday).

5.4.6 Audit Collection System (Internal vs. External)

1. Automated Audit data is generated and recorded at the application, network, and operating system level. Manually generated Audit data is recorded by NBN Co personnel.

5.4.7 Notification to Event-Causing Subject

1. Where an event is logged by the Audit collection system, no notice is required to be given to the individual, organisation, device, or application that caused the event.

5.4.8 Vulnerability Assessments

1. Events in the Audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments (LSVAs) are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a weekly basis. An annual LSVA will be an input into an entity's annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

1. NBN Co archives:
    a. All Audit data collected in terms of Section 5.4
    b. Certificate application information.
    c. Documentation supporting Certificate applications.
    d. Certificate lifecycle information, e.g., revocation, re-key, and renewal application information.

5.5.2 Retention Period of Archive

1. Records shall be retained for at least the time periods set forth below following the date the Certificate expires or is revoked:
    a. Five (5) years for Basic Assurance Certificates.
    b. Ten (10) years and six (6) months for Medium and High Assurance Certificates.

5.5.3 Protection of Archive

1. NBN Co protects the archive so that only authorised Trusted Persons can obtain access to the archive. The archive is protected against unauthorised viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the period set forth in this CPS.

5.5.4 Archive Backup Procedures

1. NBN Co incrementally backs up electronic archives of its issued Certificate information daily and performs full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Timestamping of Records

1. Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic based.

5.5.6 Archive Collection System (Internal vs. External)

1. NBN Co archive collection systems are internal.

5.5.7 Procedures to Obtain and Verify Archive Information

1. Only authorised Trusted Persons can obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

1. The NBN Co CA Key Pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. New CA Key Pair will be generated as necessary, for example to replace CA Key Pairs that are being retired, to supplement existing, active Key Pairs and to support new services.
2. Relying Parties shall be informed of the new CA issuance and are expected to make the appropriate adjustments as required.
3. Prior to the expiration of the CA Certificate for a Superior CA, Key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA Key Pair to new CA Key Pair(s). The NBN Co CA Key changeover process requires that:
    a. A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time where the remaining lifetime of the Superior CA Key Pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
4. Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the Stop Issuance Date, Certificates will be signed with a new CA Key Pair.
5. The Superior CA continues to issue CRLs signed with the original Superior CA Private Key until the expiration date of the last Certificate issued using the original Key Pair has been reached.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

1. Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate application data, audit data, and database records for all Certificates issued. Back-ups of CA Private Keys shall be generated and maintained in accordance with Section 6.2.4 . NBN Co maintains backups of the foregoing CA information for its own CAs, as well as the CAs of Enterprise Customers within its domain.

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

1. In the event of the corruption of computing resources, software, and/or data, the NBN Co incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, NBN Co Key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

1. Upon the suspected or known Compromise of an NBN Co CA, NBN Co infrastructure, or CA Private Key, NBN Co key compromise response procedures are enacted by the NBN Co security incident management processes. These processes will engage Information, Security, Cryptographic Business Operations, Production Services personnel, and other management representatives as necessary to assess the situation, develop an action plan, and implement the action plan with approval from the NBN Co PKIPA.
2. If CA Certificate revocation is required, the following procedures are performed:
    a. The Certificate's revoked status is communicated to Relying Parties through the NBN Co Repository in accordance with Section 4.9.9 ,
    b. Reasonable efforts will be made to provide additional notice of the revocation to all affected participants, and
    c. The CA will generate a new Key Pair in accordance with Section 4.7, except where the CA is being terminated in accordance with Section 4.9 .

5.7.4 Business Continuity Capabilities after a Disaster

1. NBN Co has implemented a disaster recovery site, which is physically separate from the NBN Co principal secure facilities. NBN Co has developed, implemented, and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.
2. Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. NBN Co's disaster recovery site has implemented the physical security protections and operational controls required by the NBN Co Security and Audit Requirements Guide to provide for a secure and sound backup operational setup.
3. In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from the NBN Co primary facility, the NBN Co disaster recovery process is initiated by the NBN Co Emergency Response Team (ERT).
4. NBN Co has the capability to restore or recover essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:
    a. Certificate issuance,
    b. Certificate revocation,
    c. Publication of revocation information, and
    d. Provision of Key recovery information for Enterprise Customers using Managed PKI Key Manager.

5. The NBN Co disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at the NBN Co primary site. NBN Co tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for Audit and planning purposes. Where possible, operations are resumed at the NBN Co primary site as soon as possible following a major disaster.
6. NBN Co maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA Private Keys are backed up and maintained for disaster recovery purposes in accordance with Section 6.2.4
7. NBN Co maintains offsite backups of important CA information for NBN Co CA's. Such information includes, but is not limited to: Certificate application data, Audit data (per Section 5.4), and database records for all Certificates issued.

5.8 CA or RA Termination

1. Should it be necessary for a NBN Co CA to cease operation, NBN Co makes a reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, NBN Co will develop a termination plan to minimise disruption to Subscribers and Relying Parties. Such termination plans may address the following, as determined by NBN Co (in its sole discretion):
    a. Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,
    b. Handling the cost of such notice,
    c. The revocation of the Certificate issued to the CA,
    d. The preservation of the CA's archives and records for the time periods required in this CPS,
    e. The continuation of Subscriber and customer support services,
    f. The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
    g. The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
    h. Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
    i. Disposition of the CA's Private Key and the hardware tokens containing such Private Key, and
    j. Provisions needed for the transition of the CA's services to a successor CA.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

1. CA Key Pair generation is performed by multiple pre-selected, trained, and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated Keys. The Cryptographic Modules used for CA Key generation meet the requirements of at least FIPS 140-2 level 3.
2. All CA Key Pairs are generated in pre-planned Key Generation Ceremonies, the activities performed in each Key Generation Ceremony are recorded, dated, and signed by all individuals involved. These records are kept for Audit and tracking purposes for a length of time deemed appropriate by NBN Co management.

3. Generation of RA Key Pairs is generally performed by the RA using a FIPS 140-2 level 2 certified Cryptographic Modules provided with their browser software.
4. The NBN Co generates the Key Pairs used by their NBN Co Automated Administration servers. NBN Co recommends that Automated Administration server Key Pair generation be performed using a FIPS 140-2 level 2 certified Cryptographic Module.
5. Generation of end-user Subscriber Key Pairs is generally performed by the Subscriber.

6.1.2 Private Key Delivery to Subscriber

1. When end-user Subscriber Key Pairs are generated by the end-user Subscriber, Private Key delivery to a Subscriber is not applicable.
2. Where RA or end-user Subscriber Key Pairs are pre-generated on hardware tokens or smart cards, such devices are distributed to the RA or end-user Subscriber using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged.

6.1.3 Public Key Delivery to Certificate Issuer

1. End-user Subscribers and RAs submit their Public Key for certification electronically using a PKCS #10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by TLS (Transport Layer Security), where CA Key Pairs are generated by NBN Co, this requirement is not applicable.

6.1.4 Key Sizes

1. Key pairs shall be of sufficient length to prevent others from determining the Key Pair's Private Key using cryptanalysis during the period of expected utilisation of such Key Pairs. The current NBN Co Standard for minimum Key sizes is the use of Key Pair's equivalent in strength to 4096-bit RSA for NBN Co Root and Intermediate CAs and at least 2048-bit RSA for Issuing CAs.
2. NBN Co recommends that Registration Authorities and end-user Subscribers generate minimum 2048-bit RSA Key Pairs. NBN Co may not approve certain End Entity Certificates generated with a Key Pair size of less than 2048-bits.

6.1.5 Public Key Parameters Generation and Quality Checking

1. Not applicable.

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

1. Refer to the Certificate Policy.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

1. NBN Co has implemented a combination of physical, logical, and procedural controls to ensure the security of CA Private Keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorised use of Private Keys.

6.2.1 Cryptographic Module Standards and Controls

1. For CA Key Pair generation and CA Private Key storage, NBN Co uses hardware Cryptographic Modules that are certified at or meet the requirements of FIPS 140-2 Level 3.

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

1. NBN Co has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. NBN Co uses:
    a. Secret Sharing to split the Activation Data needed to make use of a CA Private Key into separate parts named Secret Shares which are held by trained and trusted individuals named Shareholders. A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a hardware Cryptographic Module (n) is required to activate a CA Private Key stored on the module.
2. The threshold number of shares needed to sign a CA Certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

1. CA Private Keys are not escrowed. Escrow of Private Keys for end user Subscribers is explained in more detail in the Certificate Policy.

6.2.4 Private Key Backup

1. NBN Co creates backup copies of CA Private Keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware Cryptographic Modules and associated key storage devices. Cryptographic Modules used for CA Private Key storage meet the requirements of this CPS. CA Private Keys are copied to backup hardware Cryptographic Modules in accordance with this CPS.
2. Modules containing onsite backup copies of CA Private Keys are subject to the requirements of this CPS. Modules containing disaster recovery copies of CA Private Keys are subject to the requirements of this CPS.
3. NBN Co does not store copies of RA Private Keys. For the backup of end-user Subscriber Private Keys, see Section 6.2.3 and Section 4.12

6.2.5 Private Key Archival

1. Upon expiration of an NBN Co CA Certificate, the Key Pairs associated with the Certificate will be securely retained for a period of at least 5 years using hardware Cryptographic Modules that meet the requirements of this CPS. These CA Key Pairs shall not be used for any signing events after their expiration date, unless the CA Certificate has been renewed in terms of this CPS.
2. The NBN Co does not archive copies of RA and Subscriber Private Keys.

6.2.6 Private Key Transfer into or From a Cryptographic Module

1. NBN Co generates CA Key Pairs on the hardware Cryptographic Modules in which the keys will be used. In addition, NBN Co makes copies of such CA Key Pairs for routine recovery and disaster recovery purposes. Where CA Key Pairs are backed up to another hardware Cryptographic Module, such Key Pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

1. CA or RA Private Keys held on hardware Cryptographic Modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

1. All participants shall protect the Activation Data for their Private Keys against loss, theft, modification, unauthorised disclosure, or unauthorised use.

6.2.8.1 Basic Assurance Certificates

1. The Standard for Basic Assurance Private Key protection is for Subscribers to take reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated Private Key without the Subscriber's authorisation. In addition, the NBN Co recommends that Subscribers use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the Private Key, which includes, for instance, a password to operate the Private Key, a Windows logon or screen saver password, or a network logon password.

6.2.8.2 Medium Assurance Certificates

1. The Standard for Medium Assurance Private Key protection is for Subscribers to:
    a. Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the Private Key, which includes, for instance, a password to operate the Private Key, a Windows logon or screen saver password, a network logon password; and
    b. Take reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated Private Key without the Subscriber's authorisation.
2. When deactivated, Private Keys shall be kept in encrypted form only.

6.2.8.3 PKI Service Administrator Certificates

1. The Standard for Private Key protection (other than Administrators) is for Subscribers to:
    a. Use a smart card, biometric access device, password, or security of equivalent strength to authenticate the Subscriber before the activation of the Private Key; and
    b. Take reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated Private Key without the Subscriber's authorisation.
2. Use of a password along with a smart card or biometric access device in accordance with Section 6.1.1 is recommended. When deactivated, Private Keys shall be kept in encrypted form only.

6.2.8.4 Administrators' Private Keys

1. The Standard for Administrators' Private Key protection requires them to:
    a. Use a smart card, biometric access device, password in accordance with Section 6.4.1 , or security of equivalent strength to authenticate the Administrator before the activation of the Private Key, which includes, for instance, a password to operate the Private Key, a Windows logon or screen saver password, or a network logon password; and
    b. Take reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated Private Key without the Administrator's authorisation.
2. NBN Co recommends that Administrators use a smart card, biometric access device, or security of equivalent strength along with the use of a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the Private Key.
3. When deactivated, Private Keys shall be kept in encrypted form only.

6.2.9 Method of Deactivating Private Key

1. NBN Co CA Private Keys are deactivated upon removal from the token reader. NBN Co RA Private Keys (used for authentication to the RA application) are deactivated upon system log off. NBN Co RAs are required to log off their workstations when leaving their work area.
2. Client Administrators, RA, and end-user Subscriber Private Keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers has an obligation to adequately protect their Private Key(s) in accordance with this CPS. The Private Key associated with an application is deleted immediately after it has been used for code signing.

6.2.10 Method of Destroying Private Key

1. Where required, NBN Co destroys CA Private Keys in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key. NBN Co utilises the zeroing function of its hardware Cryptographic Modules and other appropriate means to ensure the complete destruction of CA Private Keys. CA key destruction activities are logged.

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. NBN Co CA, RA, and end-user Subscriber Certificates are backed up and archived as part of NBN Co routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

1. Refer to the Certificate Policy and the NBN Co PKI framework.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

1. Activation Data (Secret Shares) used to protect tokens containing NBN Co CA Private Keys is generated in accordance with the requirements of Section 6.2.2 . The creation and distribution of Secret Shares is logged.

6.4.2 Activation Data Protection

1. NBN Co Secret Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

1. To the extent Activation Data for Private Keys are transmitted, NBN Co PKI Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorised disclosure, or unauthorised use of such Private Keys. To the extent System or network logon username/password combination is used as Activation Data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorised users.

6.4.3.2 Activation Data Destruction

1. Activation Data for CA Private Keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorised disclosure, or unauthorised use of the Private Keys protected by such Activation Data. After the record retention periods in Section 5.5.2 lapse, NBN Co shall decommission Activation Data by overwriting and/or physical destruction.

6.5 Computer Security Controls

1. NBN Co performs all CA and RA functions using Trustworthy Systems that meet the requirements of NBN Co Security and Audit Requirements.

6.5.1 Specific Computer Security Technical Requirements

1. NBN Co ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorised access. In addition, NBN Co limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.
2. The NBN Co production network is logically separated from other components. This separation prevents network access except through defined application processes. NBN Co uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.
3. NBN Co requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. NBN Co requires that passwords be changed on a periodic basis.
4. Direct access to NBN Co databases supporting NBN Co CA Operations is limited to Trusted Persons in the hosted Production Operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

1. A version of NBN Co core Processing Centre software has satisfied the EAL 4 assurance requirements of *ISO/IEC 15408-3:1999, Information technology - Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*, based on an independent laboratory's Common Criteria evaluation of the software against the NBN Co Processing Centre Security Target. NBN Co may, from time to time, evaluate new releases of the Processing Centre software under the Common Criteria.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

1. Applications are developed and implemented by NBN Co in accordance with NBN Co systems development and change management standards.

2. Such developed software, when first loaded, provides a method to verify that the software on the system originated from NBN Co, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

1. NBN Co has mechanisms and/or policies in place to control and monitor the configuration of its CA systems.
2. The configuration, including modifications and upgrades of NBN Co PKI components shall be documented.
3. There shall be a mechanism for detecting unauthorised modification to the software or configuration of NBN Co PKI components.
4. The NBN Co Issuing Certification Authorities must only have applications or component software, or hardware installed that are directly related to the operation of the NBN Co PKI.

6.6.3 Life Cycle Security Controls

1. Equipment (hardware and software), including modifications and upgrades, procured for the NBN Co PKI shall be:
    a. purchased through a mechanism that will reduce the likelihood that any component was tampered with;
    b. shipped or delivered via controlled methods that provide a continuous chain of accountability from its origin to its destination and handover to NBN Co;
    c. deployed using NBN Co authorised personnel.

6.7 Network Security Controls

1. NBN Co performs all its CA and RA functions using networks secured in accordance with the NBN Co Security and Audit Requirements to prevent unauthorised access and other malicious activity. NBN Co protects its communications of sensitive information using encryption and Digital Signatures.

6.8 Timestamping

1. Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic based.
2. A trusted source of network time shall be used.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

1. Refer to the Certificate Policy.

7.2 CRL Profiles

1. Refer to the Certificate Policy.

7.3 OCSP Profiles

1. Refer to the Certificate Policy.

8. Compliance Audit and Other Assessments

1. The NBN Co shall be entitled to perform audits, reviews and investigations to ensure the trustworthiness of the NBN Co PKI, which include, but are not limited to:
    a. NBN Co shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" in the event NBN Co has reason to believe that the audited entity has failed to meet NBN Co PKI Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the NBN Co PKI.
    b. NBN Co shall be entitled to perform "Supplemental Risk Management Reviews" following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.
2. NBN Co shall be entitled to delegate the performance of these Audits, reviews, and investigations to a third-party Audit firm. Entities that are subject to an Audit, review, or investigation shall provide reasonable cooperation with NBN Co and the personnel performing the Audit, review, or investigation.

8.1 Frequency or Circumstances of Assessment

1. Audits are conducted at least annually at the sole expense of the audited entity.

8.2 Identity/Qualifications of Assessor

1. Refer to the Certificate Policy.

8.3 Assessor's Relationship to Assessed Entity

1. Refer to the Certificate Policy.

8.4 Topics Covered by Assessment

1. Refer to the Certificate Policy.

8.5 Actions Taken as a Result of Deficiency

1. Refer to the Certificate Policy.

9. Other Business and Legal Matters

9.1 Fees

1. Refer to the Certificate Policy.

9.2 Confidentiality

1. Refer to the Certificate Policy.

9.3 Privacy

1. Refer to the Certificate Policy.

9.4 Intellectual Property Rights

1. Refer to the Certificate Policy.

9.5 Term and Termination

9.5.1 Term

1. The CPS becomes effective upon publication in the NBN Co Repository and continues to be effective until terminated in accordance with Section 9.5.2 below. Amendments to this CPS become effective upon publication in the NBN Co Repository.

9.5.2 Termination

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

9.5.3 Effect of Termination and Survival

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

9.6 Individual Notices and Communications with Participants

1. Unless otherwise specified by agreement between the parties, NBN Co PKI participants shall use reasonable methods to communicate with each other, considering the criticality and subject matter of the communication.

9.7 Amendments

9.7.1 Procedure for Amendment

1. Amendments to this CPS may be made by the NBN Co PKIPA for any reason at any time in its discretion by publication of the amended CPS in accordance with paragraph 2 below.
2. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be available from the NBN Co PKI Repository located under https://pki.nbnco.net.au/CPS. Such amendments will be effective immediately upon publication by NBN Co.
3. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.
4. The NBN Co PKIPA may, from time to time and in its sole discretion, consult with NBN Co PKI Participants regarding proposed amendments to the NBN PKI. If, following consultation with NBN Co PKI Participants, the NBN Co PKIPA considers an amendment to be desirable and proposes to implement the amendment, the NBN Co PKIPA will amend the CPS and notify the NBN Co Participants in accordance with this Section 9.7

9.7.2 Circumstances under Which OID Must Be Changed

1. If the NBN Co PKIPA determines that a change is necessary in the object identifier corresponding to a Certificate Policy, the amendment shall contain new object identifiers for the Certificate Policies. Otherwise, amendments shall not require a change in Certificate Policy object identifier.

9.8 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 NBN Co PKI Participants irrevocably submit to the non-exclusive jurisdiction of courts with jurisdiction in the State of NSW, Australia, and waive any right to object to the venue on any ground.

9.9 Compliance with Applicable Law

1. All NBN Co PKI Participants agree to abide by the provisions of all relevant legislation, binding rules and codes, and the requirements of any applicable Commonwealth, State, Territory, or local government agency.

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, that 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.
Assurance Level	A specified level of assurances as defined within the CP.
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.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
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.
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.
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.
Hardware Security Module	A hardware device incorporating tamper protection, used to securely generate and store cryptographic keys.
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	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property 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 maintained 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 maintained online so as 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 promulgating 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
SSL	Secure Sockets Layer
TLS	Transport Layer Security