Philippine National Public Key Infrastructure (PKI)

Certification Practice Statement version 1.0

Version: 1.0
Effective: December 23, 2013

Philippine National PKI Certificate Practice Statement

Content

Purpose

This Certification Practice Statement (CPS) states the practices that the PNPKI CA employs in providing certification services in accordance with the specific requirements of the PNPKI Certificate Policy version 1.0.

Scope

This document applies to Certification Authorities that issue the following: (1) general purpose certificate, which can be used for all government and private transactions; (2) specific purpose certificate, which can only be used for a specific transaction; and (3) SSL certificate, which is used to encrypt the data that moves between two computers.

Issuing Authority

This document has been compiled and issued by the DOST-ICT Office and DOST-Advance Science and Technology Institute (ASTI), through the Integrated Government Philippines (iGovPhil) Project.

Contact Information

Associated publications under iGov Philippines Project can be found at http://i.gov.ph. Specific information related to the PNPKI can also be found at http://i.gov.ph/index.php/services/public-key-infrastructure-pki/.

Queries, suggestions and clarifications with regard to this document may be forwarded to pki@icto.dost.gov.ph.

1. Introduction

The Certificate Policy describes what needs to done and the policies around this. The Certification Practice Statement (to be referred to as “CPS” hereafter) describes the manner in which the policy statements need to be executed.

This document titled CPS has been prepared for the purpose of explaining the technical and legal requirements met by the Philippine National Public Key Infrastructure (PNPKI). The Information and Communications Technology Office is responsible of the PNPKI RootCA and its hierarchy, that includes the Government CA (GovCA) and all Issuing CAs.

The CPS contains a detailed description of the practices followed by a PNPKI CA in issuing and otherwise managing certificates. In general, CPSs also describe practices relating to all certificate lifecycle services.

This CPS has been prepared in compliance with the standards of RFC 3647.

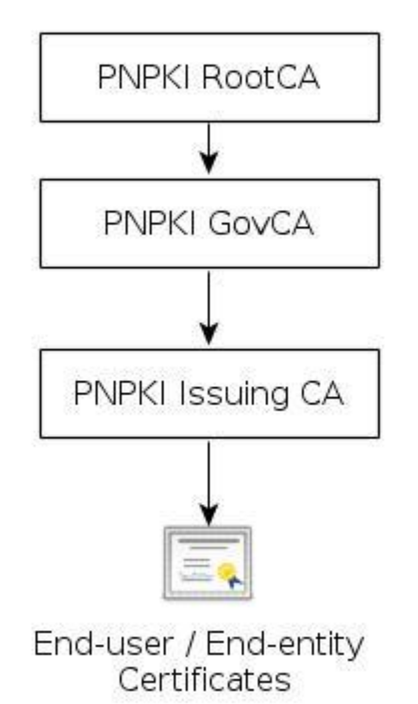
1.1Overview

The PNPKI RootCA is the trust anchor for the PNPKI hierarchy. This means that the PNPKI RootCA is self-signed. The PNPKI RootCA is used to sign other PNPKI CAs to create a PNPKI CA hierarchy.

The GovCA will act as Policy CA with several Issuing CAs signed by it. The CP/CPS will stipulate under what conditions an Issuing CA is allowed to issue certificate as well as to whom.

The PNPKI hierarchy is implemented following “best practices” and is compliant with standards, such as the CEN Workshop Agreement (CWA) and WebTrust Program for Certification Authorities.

This CPS may be used by a relying party to determine the level of trust associated with the given policy.



1.2 Document Name and Identification

This document is the PNPKI CPS. As detailed in this CPS, the PNPKI has the following issuers of digital certificates. The types of digital certificates issued are identified by the following object identifiers (OIDs):

Certification Authority	**PNPKI OID**
Philippine Root CA	2.16.608.1.2.1.1
Philippine Government CA	2.16.608.1.3.1.1
Philippine Authentication CA	2.16.608.1.4.1.1
Philippine Signing CA	2.16.608.1.5.1.1
Philippine SSL CA	2.16.608.1.6.1.1

1.3 PKI Participants

1.3.1 Certification Authorities

a) Root Certification Authority (RootCA)

The PNPKI RootCA is the primary trust point for the entire PKI architecture. The Information and Communications Technology Office-National Computer Center (ICT Office-NCC) is designated to operate a hierarchy of Philippine Certification Authorities.

Obligations of PNPKI RootCA:

i. Operate and manage the PNPKI RootCA system and its functions;
ii. Issue and manage certificates for designated Government or Accredited Private CAs (Subordinate CAs);
iii. Re-key of the Root CA and approved CA signing keys;
iv. Establishment and maintenance of the CPS;
v. Provide technical expertise in the conduct of assessment of PNPKI CAs when necessary;
vi. Support international cooperation on certification service, including mutual recognition and cross-certification;
vii. Notification of issuance, revocation or renewal of its certificates; and
viii. Resolve disputes between concerned parties.

The PNPKI RootCA servers are not reachable through the network.

b) Subordinate Certification Authorities

The subordinate CAs include the GovCA and its issuing CAs as well as Accredited Certification Authorities (ACA).

Obligations of the Subordinate CAs:

i. Operate and manage the subordinate CA system and its functions in accordance with the RootCA-CP;
ii. Issue and manage certificates for Issuing CAs; and
iii. Notification of issuance, revocation or renewal of its certificates.

Obligations of Issuing CAs:

a) Operate and manage the Issuing CA system and its functions in accordance to all applicable PNPKI CA policies;
b) Issue and manage certificates to user or juridical entities, used for general or specific purpose;
c) Publish issued certificates and revocation information;
d) Handle revocation request regarding certificate issued by the PNPKI CA; and
e) Notification of issuance, revocation or renewal of its certificates.

1.3.2 Registration Authorities

The PNPKI CA may designate specific RAs to perform the Subscriber Identification and Authentication and Certificate Request and Revocation functions defined in the CPS and related documents.

The RA shall perform certain functions pursuant to an RA Agreement including the following:

(a) Identify the user and register the user information;
(b) Transmit certificate request to the PNPKI CA;

(c) Validate certificates from the PNPKI CA Directory Server and CRL, and if available, via Online Certificate Status Protocol (OCSP); and
(d) Request revocation of certificates.

1.3.3 Subscribers

A subscriber is an individual or entity whose name appears as the subject in a certificate. The subscriber asserts that he, she or it uses the keys and certificate in accordance with the certificate policy, which include:

(a) Accuracy of representations in certificate application;
(b) Protection of the entity's private key;
(c) Restrictions on private key and certificate use; and
(d) Notification upon private key compromise.

1.3.4 Relying Parties

A relying party is the entity that relies on the validity of the subscriber’s link to a public key. The relying party is responsible for the decision to check and the manner of checking the information in the certificate. A relying party may use the information in the certificate to determine the suitability of the certificate for a particular use. Such information includes the following:

(a) Purposes for which the certificate is used;
(b) Digital signature verification responsibilities;
(c) Revocation checking responsibilities; and
(d) Acknowledgement of applicable liability caps and warranties.

A relying party may or may not be a subscriber.

1.3.5 Other Participants

1.3.5.1 Accreditation and Assessment Body

E.O. 810, s2009 mandates the Department of Trade and Industry (DTI), through its Philippine Accreditation Office (PAO), as the accreditation and assessment body for certification authorities (CAs). DTI-PAO is responsible for the functions stipulated under Section 3(d) of E.O. 810, s2009.

1.3.5.2 DTI-Bureau of Product Standards (DTI-BPS)

Collaborate with the PNPKI to develop and prescribe technical standards for digital signatures.

1.4 Certificate Usage

A subscriber shall be bound to use the certificate for its lawful and intended purposes only.

1.4.1 Appropriate Certificate Usage

(a) The PNPKI RootCA certificate can only be used for signing its CRL and the certificates of the subordinate GovCA and ACAs.
(b) Subordinate CA certificates can only be used for signing certificates, CRLs, OCSP and time stamp certificates, as well as for verification of subject certificates and data.
(c) Certificates issued by Philippine Issuing CAs can only be used strictly as part of the framework of the limitations incorporated in the certificates.

Relying parties are required to seek further independent assurances before any act of reliance is deemed reasonable and, at a minimum, must assess:

(a) The appropriateness of the use of the certificate for any given purpose and that the use is not prohibited by this CPS.
(b) That the certificate is being used in accordance with its Key-Usage field extensions.
(c) That the certificate is valid at the time of reliance by reference to OCSP or CRL.

1.4.1.1 Certificates Issued to Individuals

Individual Certificates are normally used by individuals to sign documents, encrypt e-mail and to authenticate applications (client authentication).

1.4.2 Prohibited Certificate Usage

All issued certificates under this CPS cannot be used for purposes other than what is allowed in Section 1.4.1 (Appropriate Certificate Usage) above. The certificate extensions Root CA shall not be liable for any claims arising from prohibited use.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The ICT Office-NCC is responsible for all aspects of this CPS

Philippine National PKI
ICT Office-NCC Building
Carlos P. Garcia Avenue
U.P. Campus, Diliman

1101 Quezon City, PHILIPPINES
Tel. No.: (+632) 920-0101
Fax No.: (+632) 920-7414

1.5.2 Contact Person

Office of the Executive Director
ICT Office-NCC Building
Carlos P. Garcia Avenue
U.P. Campus, Diliman
1101 Quezon City, PHILIPPINES
E-Mail: pki@icto.dost.gov.ph
Tel. No.: (+632) 920-0101
Fax No.: (+632) 920-7414

1.5.3 Person Determining CPS Suitability for the Policy

Under Section 4.4 of DTI Department Administrative Order No. 10-09, series of 2009 (DTI-DAO No. 10-09, s2009), the Certification Practice Statement (CPS) is one of the assessment requirements by the DTI-PAO.

Philippine Accreditation Office
3/F Trade and Industry Building
361 Sen. Gil J. Puyat Avenue
Makati City
E-Mail: pao@dti.gov.ph
Tel. No.: (+632) 751-3127 to 28
Fax No.: (+632) 751-3262

1.5.4 Approval Procedures

A PNPKI CA operating under this CPS shall follow the CPS approval process issued by DTI-PAO as part of the assessment requirements under DTI-DAO No. 10-09, s2009.

1.6 Definitions and Acronyms

All definitions, acronyms and abbreviations are found at:

Appendix A – Acronyms and Abbreviations
Appendix B – Definitions

2. Publication and Repository Responsibilities

2.1 Repositories

The PNPKI RootCA, Philippine GovCA and ACAs are responsible for maintaining publicly accessible online repository.

The PNPKI publishes its CP, CPS and the subscriber agreement in the official repository at_http://govca.npki.gov.ph/repository.html. Any revocation data on issued digital certificates is published at location of the CRL distribution point or OCSP responder specified in the certificate.

2.2 Publication of Certification Information

All issued certificate will be stored in the LDAP Directory. The LDAP Directory is accessible at ldap.npki.gov.ph.

2.3 Frequency of Publication

Updates to this CPS are published in accordance with Section 9.12 (Amendments). A certificate shall be published in repositories as soon as it is issued, renewed or revoked. Certificate status information is published in accordance with the provisions of this CPS.

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for PNPKI CA Certificates are issued quarterly or whenever a PNPKI CA Certificate is revoked. The CRL issuing process is automatic and is based on a daily issuing cycle.

This CPS and any subsequent changes shall be made publicly available within three (3) calendar days after its approval.

2.4 Access Controls on Repositories

The information published in the repository of the PNPKI site is publicly accessible. Read-only access to such information is unrestricted. The PNPKI CA shall protect information not intended for public dissemination or modification.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The PNPKI CA Certificates contain an X.501 Distinguished Name (DN) in the Issuer and Subject fields and consist of the components below:

Attribute	Value
Common Name (CN)	This attribute includes the CA Name
Organization (O)	"DOST"
Country (C)	"PH"

Subscriber Certificates contain an X.501 Distinguished Name (DN) in the Subject name field and consists of the components below:

Attribute	Value
Common Name (CN)	This attribute may include: • Name of individual (for certificates issued to individuals) • Organization name (for certificates issued to juridical entity) • Domain name (for server certificates)
Organizational Unit (OU)	Such attributes may contain one or more of the following: • Subscriber organizational unit • Text to describe the type of Certificate • Text to describe the entity or agency • A validated domain
Organization (O)	The Organization attribute is used as follows: • Subscriber organizational name for server certificates • Individual certificates that have an organization affiliation, or • A domain name, or verified site
Country (C)	"PH"

3.1.2 Need for Names to be Meaningful

Names used in the certificates must be in a form commonly understood semantically to determine the identity of a person and/or organization. A name is meaningful only if it can be understood and used by Relying Parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

The PNPKI CAs operating under this CPS shall not issue anonymous certificates. Pseudonymous certificates may be issued under this CPS only to support internal operations.

3.1.4 Rules for Interpreting Various Name Forms

The naming convention used by PNPKI RootCA and its subordinate CAs is ISO/IEC 9595:1998 (X.500) Distinguished Name (DN).

3.1.5 Uniqueness of Names

The Issuing CA ensures that the Subject Distinguished Name (DN) of a subscriber is unique within the domain of a specific CA through automated components of the TMS-RA enrollment process. It is possible for a subscriber to have two or more certificates with the Subject DN.

3.1.6 Recognition, Authentication and Role of Trademarks

Certificate applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. The PNPKI, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate or otherwise resolve any dispute concerning the ownership of any domain name, trade name, or trademark. The PNPKI 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 of Proof of Possession of Private Key

In all cases where the subject named in a certificate generates its own keys, that subject shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

In the case where key generation is under the PNPKI CA or RA’s direct control, proof of possession is no longer required.

3.2.2 Authentication of Organization Identity

Requests for the PNPKI CA certificates shall include the CA name, address and documentation of the existence of the organization.

The PNPKI RootCA or subordinate CA shall verify the information, in addition to the authenticity of the requesting representative and the representative’s authorization to act in the name of the PNPKI CA.

Juridical applicant’s information shall be verified with prior submission of the following:

a) Tax Payer Identification Number (TIN);
b) Authorization Letter/Board Resolution naming the authorized representative/s to apply for a digital certificate in behalf of the agency;

c) Consent to verify the information submitted;
d) Verified e-mail address owned by the organization or authorized by the owner of the e-mail address to be used by the organization; and
e) Latest copy of a bill showing the physical address of the applicant, where the PIN which will be used to activate a digital certificate shall be mailed;

For a government agency:

f) Government Service Insurance System (GSIS) registration number;

For non-government entities:

g) Securities and Exchange Commission (SEC) business registration for corporation and partnership, DTI Certificate of Business Name Registration for single proprietorship or Cooperative Development Authority (CDA) registration for cooperatives;
h) Business Permit issued by the Local Government Unit (LGU); and
i) Social Security System (SSS) Employer Clearance;

For organizations requesting SSL certificates, the following requirements shall be followed:

(a) Authorization letter, signed by the head of the organization, naming the authorized representative/s; and
(b) Certification from the Philippine Government Internet Domain Name Registry validating the authenticity of the entity's domain name or other recognized domain name registry operating in the Philippines recognized by the PNPKI; or, any proof of ownership of a particular domain name.

3.2.3 Authentication of Individual Identity

For subscribers or authorized representatives, the PNPKI CAs and/or its RAs shall ensure that the identity information is verified by prior compliance with the following:

(a) Personal appearance of the applicant;
(b) Tax Payer Identification Number (TIN);
(c) A Unified Multi-Purpose Identification (UMID)-compliant card. In the absence of UMID-compliant card, any two of the following cards are allowed as valid IDs based on BSP Circular 608 series of 2008:

i. Passport
ii. Driver's License
iii. Professional Regulation Commission (PRC) ID
iv. National Bureau of Investigation (NBI) Clearance
v. Police Clearance
vi. Postal ID

vii. Voter's ID
viii. Government Service Insurance System (GSIS) e-Card
ix. Social Security System (SSS) Card
x. Senior Citizen Card
xi. Overseas Workers Welfare Administration (OWWA) ID
xii. OFW ID
xiii. Seaman's Book
xiv. Alien Certification of Registration/Immigrant Certificate of Registration
xv. Government Office and GOCC ID, e.g. Armed Forces of the Philippines (AFP ID), Home Development Mutual Fund (HDMF ID)
xvi. Certification from the National Council for the Welfare of Disabled Persons (NCWDP)
xvii. Department of Social Welfare and Development (DSWD) Certification
xviii. Integrated Bar Of The Philippines ID
xix. Company IDs Issued by Private Entities or Institutions Registered with or Supervised or Regulated either by the BSP, SEC or IC

(d) A passport-size photo taken within the last six (6) months;
(e) Phone number (mobile and/or landline);
(f) E-mail address owned by the individual or authorized by the owner for use by the subscriber;
(g) Latest copy of a bill showing the physical address of the applicant where the PIN, which will be used to activate a digital certificate, shall be mailed; and
(h) Consent to verify the information submitted.

3.2.4 Non-Verified Subscriber Information

Any information that is not verified shall not be included in certificates.

The PNPKI does not confirm non-DNS-addressable pseudodomains and host names that can only be used internally within the Subscriber's network (e.g., mailserver.domain.local, mail, company.local, etc.).

3.2.5 Validation of Authority

Before issuing PNPKI CA certificates or signature certificates that assert organizational authority, the PNPKI CA shall validate the individual's authority to act in the name of the organization.

Whenever an individual's name is associated with an organization name in a certificate that indicate the individual's affiliation or authorization to act on behalf of the organization, the PNPKI CA or an RA:

- Determines that the organization exists by using at least one third party identity proofing database or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization.

3.2.6 Criteria for Interoperation

The ICT Office-NCC, through PNPKI RootCA, shall allow inter-operation of a non-PNPKI CA in circumstances where the PNPKI CA at a minimum:

a) Enters into a contractual agreement with the PNPKI;
b) Operates under CPS that meets the PNPKI requirements for the certificates it issues;
c) Passes the compliance assessment before being allowed to inter-operate;
d) Passes an annual compliance assessment for ongoing eligibility to inter-operate.

3.3 Identification and Authentication for Re-Key Request

Prior to the expiration of an existing certificate, the subscriber needs to obtain a new certificate to maintain continuity of Certificate Usage. Subscribers have the option of generating a new Key Pair to replace the expiring Key Pair (technically defined as “re-key”) or of creating a new Certificate Signing Request (CSR) for an existing Key Pair (technically defined as “renewal”).

Generally speaking, both “Re-key” and “Renewal” are commonly described as “Certificate Renewal,” focusing on the fact that the old certificate is being replaced with a new certificate and a new key pair generated.

Renewal of certificates shall follow the same steps as that of the initial issuance of a certificate.

3.3.1 Identification and Authentication for Routine Re-Key

The PNPKI CA certificate re-key follows the same procedure as that of the initial key generation.

Subscriber certificates shall not be subject for re-key. A new certificate with new keys shall be generated based on initial issuing process.

3.3.2 Identification and Authentication for Re-Key after Revocation

After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process described in Section 3.2 (Initial Identity Validation) above to obtain a new certificate with new keys.

3.4Identification and Authentication of Revocation Request

The PNPKI organization is responsible for authenticating all revocation requests to all PNPKI CAs based on the following requirements:

(a) Confirmation that the person making the revocation request is the subscriber or the request is done by the authorized representative of the subscriber;
(b) Immediately upon revocation, publish a signed notice of the revocation or a CRL in all repositories of such list;
(c) Requests for revocation shall be received and acted upon at all times of the day and on all days of the year; and
(d) Record and keep, in trustworthy manner, the reason for revocation, the date and time of all transactions in relation to the revocation request.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Applications

Only accredited PNPKI CAs can be signed by PNPKI Root CA. The accreditation itself will be performed by DTI-PAO.

An application for a certificate shall be made directly with a CA operating under this CPS or through its accredited RA and fulfilling the application requirements as enumerated in Section 3 (Identification and Authentication) of this CPS.

4.1.1 Who Can Submit Certificate Application

Below is a list of people who can submit certificate applications:

(a) Any individual who is the subject of the certificate;
(b) Any authorized representative of a juridical entity or organization;
(c) Any authorized representative of a CA; or
(d) Any authorized representative of an RA.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Subscriber Certificates shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties and undergo the following enrolment process:

a) Submission of a duly accomplished application form;
b) Application and verification;
c) Approval by trusted RA administrator; and
d) Downloading of the digital certificate.

4.1.2.2 CA and RA Certificates

Subscribers of the PNPKI CA and RA Certificates enter into a contract with PNPKI. The PNPKI CA and RA applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process.

4.2 Certificate Application Processing

The PNPKI will verify that the information in the Certificate Application Form is accurate before a certificate is issued.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of an applicant for a certificate must meet the requirements specified in Section 3.2 (Initial Identity Validation) of this CPS.

The PNPKI CA or an RA shall identify and authenticate all required subscriber information in terms of Section 3.2 (Initial Identity Validation).

4.2.2 Approval or Rejection of Certificate Application

The PNPKI has the right to reject an application if requirements provided in this CPS are not complied with. Otherwise, the application is deemed approved. Applicants whose applications have been rejected may subsequently re-apply.

4.2.3 Time to Process Certificate Application

PNPKI CA begins processing certificate application within a reasonable time of receipt. There is no time stipulation to complete the processing of an application. A certificate application remains active until rejected.

4.3 Certificate Issuance

Any PNPKI CA operating under this CPS shall follow the requirements of Section 12.4 of DTI-DAO No. 10-09 for certificate issuance.

When certificates are issued to the PNPKI CAs (Subordinate CAs), the PNPKI is responsible for performing of all necessary validation.

For all end-user certificates, the RA shall conform to the requirements of Section 12.4 of DTI Department Administrative Order No. 10-01 (DTI DAO No. 10-09) issued on 29 September 2010 for digital certificate issuance.

4.3.1 CA Actions During Certificate Issuance

A certificate is created and issued following the approval of an Application for Digital Certificate by PNPKI CA or following receipt of an RA's request to issue the Certificate. The PNPKI CA creates and issues to an applicant a certificate based on the information provided in the approved Application for Digital Certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The PNPKI CAs shall, either directly or through an RA, notify end-user subscribers that they have created such certificates and provide them access to the certificates. They shall be allowed to download the certificate from a website.

4.4 Certificate Acceptance

Before an end-user subscriber can make effective use of the private key, the PNPKI CA/RA shall detail the subscriber's responsibilities as defined in Section 9.6.3 (Subscriber Representations and Warranties) of this CPS.

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

a) A certificate shall be deemed accepted when it is in the subscriber or a representative's control;
b) Failure of the subscriber to object to the certificate or its content within five (5) calendar days; or
c) The subscriber uses the certificate.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2 (Publication and Repository Responsibilities) of this CPS, all certificates shall be published in the CA's repository system.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

A PNPKI CA/RA operating under this CPS may choose to notify other PNPKI CAs or RAs of the certificate issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

An end-user subscriber shall protect their private keys from access by third parties. Subscriber shall use private keys in accordance with the key usage field extension.

End-user subscriber shall be bound to use the certificate for its lawful and intended purposesonly.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate against the relevant CRL or OCSP response published by the PNPKI.

4.6 Certificate Renewal

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key and shall follow the requirements of Section 12.5 of DTI-DAO No. 10-09, s2009. Only valid certificates can be renewed.

4.6.1 Circumstances for Certificate Renewal

A PNPKI CA certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised and the Subscriber name and attributes are unchanged.

End-user Subscriber certificates shall not be subject for renewal. A new certificate with new keys shall be generated based on initial issuing process.

4.6.2 Who May Request Renewal

Authorized representatives of PNPKI CAs may request for renewal of their CA certificates directly with the PNPKI RootCA.

End-user certificates shall not be subject for renewal.

4.6.3 Processing Certificate Renewal Request

The PNPKI shall process requests for renewal by verifying that the Subscriber information has not changed. An estimation of the validity time left of the keys will be considered before the validity time of the new certificate is set.

End-user certificates shall not be subject for renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

When renewal of a certificate for a PNPKI CA (Sub CA or Issuing CA), an authorized representative will be present during certificate issuance. The notification of issuance will be immediately after certificate is signed.

Notification of issuance of certificate renewal to the end-user Subscriber is in accordance with Section 4.3.2 (Notification to Subscriber by the CA of Issuance of Certificate).

4.6.5 Conduct Constituting Acceptance of Renewed Certificate

Conduct constituting Acceptance of a renewed certificate is in accordance with Section 4.1.1 (Who Can Submit Certificate Application).

4.6.6 Publication of Renewal Certificate by the CA

As specified in Section 2 (Publication and Repository Responsibilities) of this CPS, all renewed certificates issued shall be published in the PNPKI CA's repository system.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

A PNPKI CA/RA operating under this CPS may choose to notify other PNPKI CAs or RAs of the certificate issuance.

4.7 Certificate Re-Key

Re-keying a certificate means to request a new certificate with the same certificate contents except for a new Public Key. Only valid certificates can be re-keyed. All re-keys are done manually.

4.7.1 Circumstances for Re-Key

Prior to the expiration of an existing certificate, a certificate may renew its keys if it deemed necessary regarding to one of the following reasons:

a) Migration of hardware;
b) The keys have to low cryptographic strength;
c) The keys have high exposure; or
d) Enforced by standards or applications.

A certificate may also be re-keyed after expiration. It´s within the responsible of PNPKI to accept or reject any request for re-key from other PNPKI CAs.

End-user Subscriber certificates shall not be subject for re-key. A new certificate with new keys shall be generated based on initial issuing process.

4.7.2 Who May Request for Re-Key

Authorized representatives of PNPKI CAs may request for re-key of their PNPKI CA certificates directly with the PNPKI.

End-user Subscriber certificates shall not be subject for re-key. A new certificate with new keys shall be generated based on initial issuing process.

4.7.3 Processing Certificate Re-Keying Requests

All re-key requests shall follow the same processes and procedures as when initial keys where generated.

4.7.4 Notification of New Certificate Issuance to Subscriber

PNPKI CA/RA operating under this CPS may inform the Subscriber of the issuance of re-keyed certificates as specified in Section 4.3.2 (Notification to Subscriber by the CA of Issuance of Certificate) of this CPS.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting acceptance of a re-keyed certificate is in accordance with Section 4.4.1 (Conduct Constituting Certificate Acceptance).

4.7.6 Publication of the Re-Keyed Certificate by the CA

As specified in Section 2 (Publication and Repository Responsibilities) of this CPS, all certificates shall be published in the PNPKI CA’s repository system.

4.7.7 Notification of Certificate Issuance to Other Entities

A PNPKI CA/RA operating under this CPS may choose to notify other CAs or RAs of the certificate issuance.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

a) Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the end-user Subscriber’s public key). Certificate modification is considered a Certificate Application as stated in Section 4.1 (Certificate Application).

b) Certificate modification is performed when change occurs in any of the information of an existing certificate. After modification, the original certificate shall be revoked.

c) End-user Subscriber certificates shall not be subject for modification. A new certificate with new keys shall be generated based on initial issuing process.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1 (Who Can Submit A Certificate Application).

4.8.3 Processing Certificate Modification Requests

The PNPKI RA shall process requests for modification by verifying the new information that will be used in the certificate as stated in Section 3.2 (Initial Identity Validation).

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2 (Notification to Subscriber by the CA of Issuance of Certificate).

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1 (Conduct Constituting Certificate Acceptance).

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2 (Publication of Certificate by the CA).

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3 (Notification of Certificate Issuance by the CA to Other Entities).

4.9 Certificate Revocation and Suspension

All requests for certificate revocation must be authenticated by the PNPKI. Issuing CA will publish its CRL in intervals and its OCSP will be accessible at all time.

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the bind between the subject and the subject’s public key is no longer valid.

There are several circumstances under which a PNPKI CA certificate will be revoked:

a) Key Compromise - The PNPKI CA private key has been compromised
b) PNPKI CA Compromise - The PNPKI CA database has been compromised
c) The PNPKI CA is not compliant with its CP /CPS
d) Cessation Of Operation - The PNPKI CA shall cease operation

An end-user subscriber certificate can be requested for revocation under any of the following conditions:

a) When a verified request for revocation is received by PNPKI CA or RA;
b) When any of the information found in the certificate is changed or no longer applicable;

c) When the Private Key, or the media holding the Private Key, associated with the certificate is compromised;
d) When the PNPKI CA determines that the end-user entity is no longer complying with the requirements of this CPS; or
e) When the PNPKI CA has the reason to believe that the certificate was issued in a manner that is not in accordance with the procedures required by this CPS.

4.9.2 Who Can Request Revocation

An individual end-user subscriber, or a duly authorized representative, can request the revocation of its own certificate. In the case of juridical entities, a duly authorized representative of the juridical entity or organization may request the revocation of certificates issued to that organization. Only the PNPKI CA is entitled to request or initiate the revocation of the certificate issued to its own PNPKI CAs.

4.9.3 Procedure for Revocation Request

An RA will revoke a certificate upon receipt of a valid request for revocation. A request for revocation can be initiated through a telephone call, e-mail or written request letter. The authentication and verification of revocation request shall be in accordance with Section 3.4 (Identification and Authentication of Revocation Request) of this CPS.

4.9.4 Revocation Request Grace Period

No grace period is permitted once a revocation request has been verified. RAs will revoke certificates as soon as reasonably practical following verification of a revocation request.

4.9.5 Time Period for Processing Revocation Request

All certificate revocation requests shall be executed without delay.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties shall validate any presented certificate against the most updated CRL as minimum. Alternatively, relying parties may check certificate status using OCSP. PNPKI CA shall provide relying parties with information on how to find the appropriate CRL or OCSP responder to check for revocation status.

4.9.7 CRL Issuance Frequency

CRLs for PNPKI CAs shall be issued every thirty-six (36) hours or whenever a certificate is revoked.

Special purpose PNPKI CAs shall publish its CRL based on the importance to provide correct status information.

4.9.8 Maximum Latency for CRLs

The publication of CRL shall be done without any delay and shall be made available to relying parties within four (4) hours of generation.

4.9.9 Online Revocation/Status Checking Availability

Only Issuing PNPKI CAs have OCSP enabled and provided to relying parties.

4.9.10 Online Revocation Checking Requirements

A relying party must confirm the validity of a certificate via CRL or OCSP prior to relying on the certificate.

4.9.11 Other Forms of Revocation Advertisement Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

Should a private key become compromised, the related certificate shall immediately be revoked. Should the PNPKI CA private key become compromised, all certificates issued by that PNPKI CA shall be revoked.

4.9.13 Circumstances for Suspension

The PNPKI does not allow suspension.

End-user certificates shall not be subject for suspension instead a revocation shall occur.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of public certificates is available via CRL at PNPKI CA's websites and via an OCSP Responder.

4.10.2 Service Availability

Certificate Status Services are available 24x7 without scheduled interruption.

The certificate status validation service shall deliver 99.7% availability.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

An end-user subscriber may end a subscription for a PNPKI certificate by:

a) Allowing his / her / its certificate to expire without renewing or re-keying that certificate;
b) Revoking of his / her / its certificate before certificate expiration.

4.12 Key Escrow and Recovery

The private keys for each PNPKI CA certificate were generated and are stored in Hardware Security Modules (HSM) and are backed up but not escrowed.

4.12.1 Key Escrow and Recovery Policy and Practices

The PNPKI CA key-recovery is based on HSM standard key-backup where the keys in the backup are protected with encryption. All HSM backups and administrator smartcards shall be stored in a safety vault. Only persons performing trusted roles shall have the access to the safety vault.

The PNPKI does not store copies of subscriber private keys.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management and Operation Controls

This Part 5 of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use by Philippine National PKI to provide trustworthy and reliable PNPKI CA operations.

5.1 Physical Controls

All PNPKI CA equipment, including cryptographic modules, are protected from unauthorized access at all times.

Physical security control has been applied to all PNPKI CAs and any remote workstations used to administer the PNPKI CA system, except where specifically noted.

5.1.1 Site Location and Construction

The location and construction of the facility housing the PNPKI CA equipment, as well as sites housing remote workstations used to administer the PNPKI CA systems, shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the equipment and records of PNPKI CAs.

5.1.2 Physical Access

The PNPKI CA equipment, to include remote workstations used to administer the PNPKI CA systems, shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

At a minimum, the physical access security shall:

a) Ensure that no unauthorized access to the hardware is permitted;
b) Be manually or electronically monitored for unauthorized intrusion at all times;
c) Ensure that an access log is maintained and inspected periodically;
d) Require two-person physical access control; and
e) Ensure that all removable media and paper copies containing sensitive plain-text information are stored in secure containers.

Access to the controlled area is gained by using a multilayer access system, which uses a combination of access cards and fingerprint recognition.

Any third party individual who needs to execute any operation that may affect the core certification system is considered to be in a trusted position.

5.1.3 Power and Air Conditioning

The PNPKI CA environment shall have backup capability sufficient to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. In addition, directories (containing issued certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of one (1) hour operation in the absence of commercial power.

5.1.4 Water Exposures

The PNPKI CA equipment shall be installed where it is not in danger of exposure to water.

Water exposures from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

The PNPKI CA shall implement reasonable precautions to prevent and extinguish fires in compliance with the Revised Fire Code of the Philippines (R.A. 9514).

5.1.6 Media Storage

All media storage shall be protected from accidental damage (e.g. water, fire, electromagnetic) and from unauthorized physical access.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned or otherwise rendered unrecoverable.

5.1.8 Off-Site Backup

Full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location separate from the PNPKI CA's equipment, including CRL, for 10 years after the corresponding certificates are voided. The backup shall be stored at a site with physical and procedural controls commensurate to the operational controls of the CA. A separate document describes the backup procedure of the PNPKI CA system.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is assigned to people who are extraordinarily responsible; otherwise the integrity of the PNPKI CA or RA is weakened. A trusted role's functions can introduce security problems if not carried out properly, accidentally or maliciously.

The functions performed in these roles form the basis of trust for all uses of the Philippine certification scheme for digital signatures. Approaches shall be taken to increase the likelihood that these roles can be successfully carried out. The first shall ensure that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. The following are trusted roles:

Security Officer	Has overall responsibility for administering the implementation of the security policies and practices.
System Administrator	Authorized to install, configure and maintain trustworthy systems, but with controlled access to security related information. This user does not have access to the PNPKI CA's web interface.
System Operator	Responsible for operating trustworthy system on a day-to-day basis. A System Operator is authorized to perform system backup and recovery.
System Auditor	Authorized to view archives and audit logs of the trustworthy system.
Database Administrator	Has privileged access to the database and can create users, databases and manipulate tables. The DBA has access during installation. During normal operations, the DBA is not allowed to log into the system.
Registration Officer	Responsible for approving end-user certificate generation, revocation and renewal.

Some roles may be combined or expanded. The roles required are further identified, with the following subsections providing a detailed description of some of the responsibilities for each role.

5.2.2 Number of Persons Required Per Task

Two or more persons are required for PNPKI CAs for the following tasks:

(a) CA key generation = Three (3) persons
(b) CA signing key activation = Two (2) persons

(c) CA private key backup = Three (3) persons

Where multiparty control for logical access is required, at least one of the participants shall be an administrator. All participants must serve in a trusted role as defined in Section 5.2.1 (Trusted Roles). Multiparty control for logical access shall not be achieved using personnel that serve in the Auditor Trusted Role.

HSM Administrators uses HSM Smartcards for authentication. The HSM itself enforces dual control based on the HSM smartcards for the different functions. The number of needed HSM-smartcards (m) of the total number of produced HSM-smartcards (n) will be:

(a) Key generation = 3 of 10
(b) Signing key activation = 2 of 10
(c) Private key backup and restore = 3 of 10

5.2.3 Identification and Authentication for Each Role

All individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity. All user authentications are based on two-factor authentication.

5.2.4 Roles Requiring Separation of Duties

Role separation may be enforced either by the PNPKI CA equipment, or procedurally, or by both means. No user shall be assigned multiple roles.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness and integrity.

All trusted roles are required to be held by Philippine citizens and in accordance with the following requirements:

a) Proof of the requisite background, qualifications as well as experience necessary to efficiently and sufficiently perform their job responsibilities; and

b) Proof of any government clearances needed to do certification services under government contracts.

5.3.2 Background Check Procedures

All PNPKI CA personnel acting in trusted roles shall, at a minimum, undergo a background investigation procedure covering the following areas:

(a) Employment
(b) Education and Certification
(c) Place of residence
(d) Law Enforcement
(e) References

The period of investigation must cover at least the last five (5) years for each area, excepting the residence check which must cover at least the last three (3) years. Regardless of the date of award, the highest educational degree shall be verified.

The background investigation shall be performed by the National Intelligence Coordination Agency (NICA) in conformance with E.O. 608, series 2007, entitled *"Establishing a National Security Clearance System for Government Personnel with Access to Classified Matters and for Other Purposes."*

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the PNPKI CA or RA shall receive comprehensive training in all operational duties they are expected to perform, including good knowledge on the following:

(a) The PNPKI CA's Certification Practice Statement;
(b) The Electronic Commerce Act of 2000;
(c) The Data Privacy Act of 2012;
(d) The Cybercrime Prevention Act of 2012; and
(e) The Rules Governing the Accreditation of CAs for Digital Signature.

In addition, personnel performing duties with respect to the operation of the PNPKI CA shall receive comprehensive training or demonstrate competence in the following areas:

(a) PNPKI CA/RA security principles and mechanisms;
(b) All PKI software versions in use by the PNPKI CA system; and
(c) Disaster recovery and business continuity procedures.

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles shall be aware of changes in the PNPKI CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are software or hardware upgrade, changes in automated security systems and relocation of equipment.

Documentation shall be maintained identifying all personnel who received retraining and the level of retraining completed.

5.3.5 Job Rotation Frequency and Sequence

Any job rotation frequency and sequencing procedures shall provide for continuity and integrity of the PNPKI CA's services.

5.3.6 Sanctions for Unauthorized Actions

Penalties shall be imposed on PNPKI CA personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the PNPKI CA or RA shall meet the personnel requirements set forth in this CPS, as applicable.

5.3.8 Documentation Supplied to Personnel

For the PNPKI CA and RA, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the PNPKI CA or RA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form or other physical mechanism shall be used.

All security audit logs, both electronic and non-electronic, shall be retained, indexed, stored, preserved and reproduced so as to be accurate, complete, legible and made available during compliance audits as required in Section 12.2 (Trustworthy record keeping and archival) of DTI DAO 10-09, series 2010.

5.4.1 Types of Events Recorded

A message from any source received by the PNPKI CA requesting an action related to the operational state of the PNPKI CA is an auditable event. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

(a) The type of event;
(b) The date and time of the event;
(c) A success or failure indicator, where appropriate; and
(d) The identity of the entity and/or operator (of the PNPKI CA or RA) that caused the event.

The following are auditable events:

5.4.1.1 System Access

The certificate serial number will be recorded in the log for system access to PNPKI CA.

The username and certificate serial number will be recorded in the log for system access to TMS-RA.

Proper authorization and approval from the management must be sought for any change or modification to the PKI system and its components. A change control form must be accomplished by the system administrator and duly signed by an immediate officer.

5.4.1.2 Physical Access

The access card number and username of PKI authorized personnel will be recorded in the log for physical access to the secured premises. Non-authorized PKI personnel like hardware vendor support engineers and maintenance staffs shall accomplish an access request form stating in detail the actions or reasons for such entry on the secured premises.

5.4.1.3 Key Generation

The keys generated within the HSMs are manually logged in the Key Ceremony Document.

Keys generated outside the HSM (certificate trust store) are automatically logged as an event in the GovCA server.

Key generation for end-users and end-entities (PKCS#12) is automatically logged in the GovCA database.

5.4.1.4 Certificate Lifecycle

The following information can be retrieved regarding the certificate lifecycle.

On the PNPKI CA server:

a) All issued certificates belonging to a user, entity or a PNPKI CA.
b) All expired certificates belonging to a user, entity, or a PNPKI CA.
c) All revoked certificates belonging to a user, entity or a PNPKI CA.

On the TMS-RA:

a) All issued certificates belonging to a user.
b) All expired certificates belonging to a user.
c) All revoked certificates belonging to a user.

5.4.1.5 Transaction Logs

Events accessing the OS will be recorded on the server.log file.

5.4.1.6 System Logs

Authentication to the platform events is recorded as system logs.

5.4.1.7 Application Logs

The following information are stored in the application log:

a) Issued certificates, time of issuance and by whom.
b) Revoked certificates, time of revocation and by whom.
c) Activated certificates, time of activation and by whom.
d) Creation of certificate profiles, time created and by whom.
e) Creation of administrators, time created and by whom.
f) Change in security levels, time modified and by whom.
g) Editing of roles and users, time modified and by whom.
h) Issuing of CRLs and time of issuance.

All security auditing capabilities of the PNPKI CA's operating system and applications required by this CPS shall be enabled. As a result, the events identified above shall be automatically recorded. Where events cannot be automatically recorded, the PNPKI CA shall implement manual procedures to satisfy this requirement.

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed monthly. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries with a more thorough investigation of any alerts or irregularities in the log.

Examples of irregularities include discontinuities in the logs and loss of audit data. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Log

A PNPKI CA audit log shall be retained as a minimum during its total lifetime.

Other audit logs such as system, physical access and transaction shall be retained on-site until reviewed. They shall also be retained for ten (10) years from the date of issuance of the certificate.

5.4.4 Protection of Audit Log

The PNPKI CA's system configuration and procedures must be implemented together to ensure that:

(a) Only personnel assigned to trusted roles have read access to the logs;
(b) Only authorized people may archive audit logs; and,
(c) Audit logs are not modified.

The person performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

Log information from the PNPKI CA application and TMS-RA are digitally signed to provide non-repudiation. The key pair used for log signing is stored in a separate slot in the HSM.

The off-site storage location for audit logs shall be a safe, secure location separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit shall be sent off-site on a monthly basis.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system should be internal to the PNPKI CA system. Automated audit processes shall be invoked at system or application startup and cease only at system or application shutdown.

5.4.7 Notification to Event-Causing Subject

This CPS imposes no requirement to provide notice that an event was audited to the individual, organization, device or application that caused the event.

5.4.8 Vulnerability Assessments

The PNPKI CA shall assess the vulnerability of its PNPKI CA system or its components annually. A routine assessment of the PNPKI CA system shall be performed regularly for evidence of any malicious activity.

5.5 Records Archival

All PNPKI CAs or RAs shall comply with their respective records retention policies in accordance with applicable laws and Section 12.2 of DTI DAO 10-09, series 2010.

5.5.1 Types of Records Archived

All PNPKI CAs shall make, and keep in a trustworthy manner, the records relating to the following:

a) Activities in issuance, renewal and revocation of certificates, including the process of identification of any person requesting a certificate from an accredited PNPKI CA;
b) The process of generating Subscribers' (where applicable) or the accredited PNPKI CA's own key pairs; and
c) Such related activity of an accredited PNPKI CA as may be determined later on by the PNPKI.

5.5.2 Retention Period for Archive

The minimum retention periods for archive data shall be ten (10) years.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to or delete the archive. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally authorized representative(s). Archive media shall be stored in a safe, secure storage facility separate from the PNPKI CA itself.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined.

5.5.4 Archive Backup Procedures

If a PNPKI CA operating under this CPS chooses to back up its archive records, the Archiving Procedure Manual shall describe how the archive records are backed up and managed.

5.5.5 Requirements for Time-Stamping of Records

PNPKI CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in compliance with the Philippine Standard Time Act of 2013 (R.A. 10535).

5.5.6 Archive Collection System (Internal or External)

Archive collection systems are internal. The PNPKI CA archive data are copied to additional media for processing. Reviewing will be done by the PNPKI CA itself.

5.5.7 Procedures to Obtain and Verify Archive Information

The procedures detailing how to create, verify, package, transmit and store archive information shall follow the Archiving Procedure Manual.

The contents of the archive shall not be released except as determined by the ICT Office-NCC, acting as the RootCA, and the DTI-PAO, acting as the accreditation and assessment body or as required by law. Records of individual transactions may be released upon request of any subscriber involved in the transaction or authorized representative(s).

5.6 Key Changeover

All PNPKI CAs shall adhere to the provision as stipulated in Section 5.6 (Key Changeover) of the PNPKI Certificate Policy version 1.0.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

To maintain the integrity of the PNPKI services, it implements data backup and recovery procedures. The PNPKI has developed a Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP). The PNPKI CA system is redundantly configured at its primary site (main site) and is mirrored with a tertiary system located at a separate, geographically diverse location (disaster recovery site) for manual failover in the event of a disaster. The DRP and BCP and supporting procedures are reviewed and tested periodically (at least once a year) and are revised and updated as needed.

At its primary facility (main site), the PNPKI maintains a fully redundant PNPKI CA system and its services. The secondary node PNPKI CA at the primary facility is readily available in the event that the primary node should cease operation.

At the mirror site (disaster recovery site), PNPKI maintains a tertiary node of PNPKI CA system that is a mirror of the primary facility (main site) for failover in the event the primary and secondary node PNPKI CAs should cease operation.

Appropriate escalation, incident investigation and incident response will ensue.

The PNPKI CA shall provide notice to the ICT Office-NCC, as RootCA, and DTI-PAO of any incident falling within the following requirements:

a) Compromise of PNPKI CA's signing key;
b) Penetration of PNPKI CA's system and network;
c) Unavailability of infrastructure; and
d) Fraudulent registration and generation of certificates, and revocation information.

If any incident above happens, the PNPKI CA shall report it to the ICT Office-NCC, as RootCA, and DTI-PAO within the next working day. All actions taken are documented and part of the incident report.

5.7.2 Computing Resources, Software and/or Data Are Corrupted

When computing resources, software and/or data are corrupted, the PNPKI CA shall respond as follows:

a) Before returning to operation, ensure that the system's integrity has been restored;
b) If the PNPKI CA signature keys are not destroyed, PNPKI CA operation shall be re-established, giving priority to the ability to generate certificate status information within the CRL issuance schedule; and
c) If the PNPKI CA signature keys are destroyed, PNPKI CA operation shall be re-established as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Entity (CA) Private Key Compromise Procedures

5.7.3.1 In the event that the PNPKI CA private key has been or is suspected to have been compromised, PNPKI CA personnel will immediately convene an emergency Incident Response Team (IRT) to assess the situation and to determine the degree and scope of the incident and take appropriate action. The following actions outline as follows:

a) Collect all information related to the incident (and if the event is ongoing, ensure that all data are being captured and recorded);
b) Begin investigating the incident and determine the degree and scope;
c) The IRT determines the course of action or strategy that should be taken (and in the case of Private Key compromise, determining the scope of certificates that must be revoked);
d) Contact law enforcement, and other interested parties and activate any other appropriate additional security measures;
e) Monitor system, continue the investigation, ensure that all data is still being recorded as evidence and make a forensic copy of data collected;
f) Isolate, contain and stabilize the system, applying any possible short-term fixes needed to return the system to a normal operating state;
g) Prepare an incident report that analyzes the cause of the incident and implement a long term solutions.

A new PNPKI CA Key Pair should be generated and a new PNPKI CA Certificate should be signed in accordance with the procedures outline in Section 6 (Technical Security Controls) of this CPS.

a) If the PNPKI CA distributes its Key in a self-signed certificate, the new self-signed certificate shall be distributed as specified in Section 6.1.4 (CA Public Key Delivery to Relying Parties) of this CPS.

b) The PNPKI CA governing body shall also investigate and report to the ICT Office-NCC and DTI what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

The PNPKI CA shall operate a backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary facility or site and mitigate the effects of any kind of natural or man-made disaster. The Disaster Recovery Plan is regularly tested, verified and updated to be operational in the event of a disaster. The PNPKI CA operations shall be designed to restore full service within six (6) hours of main site system failure.

5.8 CA or RA Termination

In the event that a PNPKI CA terminates its operation for any reason whatsoever, it shall notify the ICT Office-NCC, as RootCA, and DTI-PAO prior to termination in compliance with the requirements of Section 17.2 of DTI DAO 10-09, series 2010.

PNPKI CA or RA will provide timely notice and transfer of responsibilities to succeeding entities, maintenance or records, and remedies. Before the PNPKI CA terminates its activities, it will take the following steps:

a) Ensure that any disruption caused by the termination of an Issuing PNPKI CA is minimized;
b) Ensure that archived records of the Issuing PNPKI CA are retained;
c) Ensure that prompt notification of termination is provided to Digital Certificate Holders, Authorized Relying Parties and other relevant parties in the PNPKI;
d) Ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the time of termination is maintained; and
e) Notify relevant Government and Certification bodies under applicable laws and related regulations.

6. Technical Security Controls

The PNPKI CA private keys are protected within a hardware security module (HSM) meeting at least Level 3 of the Federal Information Processing Standard 140-2 (FIPS 140-2). Access to the HSM within the CA environment is restricted by the use of smartcard and biometric device. The HSM is always stored in a physically secure environment and subject to security controls throughout its lifecycle.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The PNPKI 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. For the Root CA, the cryptographic module used for key generation meet the requirements of FIPS 140-2 Level 3 with level 4 requirements in section “Physical Security” and EAL 4+ certified hardware. For subordinate CAs (including the Issuing CAs), the cryptographic modules used meet the requirements of at least FIPS 140-2 level 3.

All the PNPKI CA keys are generated in pre-planned Key Generation Ceremonies. The activities performed in each key generation ceremony are recorded, dated and signed by individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate.

Generation of the end-user subscriber key pairs is generally performed by the subscriber. The subscriber typically uses a FIPS 140-2 level 3 certified cryptographic module provided with the self-service portal for key generation.

The self-service portal shall be made available to the subscriber in a separate e-mail.

6.1.2 Private Key Delivery to Subscriber

If a subscriber generates his/her own key pairs, then there is no need to deliver private keys and this section does not apply.

If a PNPKI CA or RA generates the keys on behalf of the subscriber, then the private key must be delivered to the subscriber. Private keys may be delivered electronically or on a hardware security token. In all cases, the following requirements shall be met:

a) Anyone who generates a private signing key for a subscriber shall not retain any copy of the key after delivery of the private key to the subscriber.
b) The private key must be protected from activation, compromise or modification during the delivery process.
c) The subscriber shall acknowledge receipt of the private key.

The PNPKI CA or RA shall maintain a record of the subscriber acknowledgement of receipt of the private key.

6.1.3 Public Key Delivery to Certificate Issuer

End-user subscribers and RAs submit their public key to the PNPKI CA for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) in a session secured by Secure Sockets Layer / Transport Layer Security (SSL/TLS). Delivery of the public key occurs during the enrollment session where the applicant provides all certificate application details.

6.1.4 CA Public Key Delivery to Relying Parties

All PNPKI CAs in the hierarchy makes their Certificates available to Subscribers and Relying Parties through the self-service portal. The Philippine National PKI generally provides the full certificate chain (including the Issuing CA and any CAs in the chain) to the end-user or relying parties. Relying Parties may also obtain PNPKI CA Certificates containing its Public Key from the PNPKI website or by e-mail.

6.1.5 Key Sizes

The PNPKI generates and uses a 4096-bit RSA Key with Secure Hash Algorithm version 2 (SHA256) to sign Certificates and the CRLs that it issues. Subscriber's key pair is generated using 2048 or 4096-bit RSA with SHA256 algorithm.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The PNPKI CA and subscriber certificates include key usage extension fields to specify the purposes for which the certificate may be used and also to technically limit the functionality of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509 version 3 standard and is outside of the control of Philippine National PKI. Refer to Section 7.1.2.1 (Key Usage).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

All the PNPKI CAs has implemented a combination of physical, logical, and procedural controls to ensure the security protection and prevent the loss, damage, disclosure, modification or unauthorized use of their private keys.

6.2.1 Cryptographic Module Standards and Controls

For the Root CA key pair generation and PNPKI CA private key storage, the Root CA uses hardware cryptographic modules that are rated at Federal Information Processing Standard (FIPS) 140-2 Level 3.

For the subordinate CAs (including Issuing CAs) key pair generation and private key storage use hardware cryptographic modules that, at a minimum, are rated at FIPS 140-2 Level 3.

Hardware tokens for key pair generation and private key storage of end-user Subscribers shall, at a minimum, be rated at FIPS 140-2 Level 1.

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

All the PNPKI CAs has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive PNPKI CA cryptographic operations. A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a PNPKI CA private key stored on the module.

The threshold number of shares needed for key generation is 3 of 10 (where m=3 and n=10) signing key activation is 3 of 10 and private key backup and restore is 3 of 10. Re-activation of the backed-up PNPKI CA private keys requires the same multi-person participation as when performing other sensitive PNPKI CA private key operations.

6.2.3 Private Key Escrow

No private keys are escrowed.

6.2.4 Private Key Backup

The private keys of the PNPKI CAs are stored in encrypted state and access is only by multi-person control as specified in Section 6.2.2 (Private Key (m out of n) Multi-person Control) of this CPS. Backup copies of the PNPKI CAs private keys are created for routine recovery and disaster recovery purposes. The PNPKI CAs private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

All the PNPKI CAs do not store copies of subscriber private keys. Subscribers are solely responsible for backup of their private keys. For the backup of subscriber private keys, subscribers may choose to backup their keys to their hard drive.

6.2.5 Private Key Archival

When all the PNPKI CAs key pairs reach the end of their validity period, such PNPKI CA key pairs will be archived for a period of at least 10 years. Archived PNPKI CA key pairs will be securely stored using offline media. Procedural controls will prevent archived PNPKI CAs key pairs from being returned to production use. Upon the end of the archive period, the archived PNPKI CAs private keys will be securely destroyed.

The PNPKI does not archive copies of subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All the PNPKI CAs generate key pairs on the hardware cryptographic modules in which the keys will be used. In addition, copies of such PNPKI CAs key pairs for routine recovery and disaster recovery purposes are made. Where PNPKI CAs 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

Private keys held in the hardware cryptographic module are stored in an encrypted form and protected with 10 smart cards where a minimum of 3 cards are needed for decryption.

6.2.8 Method of Activating Private Key

All the PNPKI CAs shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure or unauthorized use.

All the PNPKI CA private keys are activated according to the specifications of the cryptographic hardware manufacturer and witnessed during the key generation or certificate signing ceremony.

6.2.9 Method of Deactivating Private Key

The PNPKI CA private keys are deactivated upon stopping of the CA system software. The RA private keys (used for authentication to the RA application) are deactivated upon system log off. RA administrators are required to log off their workstations when leaving their work area.

Client Administrators, RA and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system or upon removal of hardware token or software token depending upon the authentication mechanism employed by the user. In all cases, end-user subscribers have an obligation to adequately protect their private keys in accordance with this CPS.

6.2.10 Method of Destroying Private Key

The HSM device and associated backup are “zeroized” or re-initialized according to the specifications of the hardware manufacturer. This overwrites all of the data on the device. In cases when this zeroization procedure fails, the PNPKI will physically destroy the device to remove the ability to extract any private key.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All PNPKI CAs and subscribers’ public key are archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated certificates.

All certificates and corresponding keys shall have maximum validity periods (not exceeding):

Root CA	25 years
Sub CA (Government CA)	23 years
Issuing CA (Gov-Auth, Gov-Sign, Gov-SSL)	11 years
End-user Subscriber	2 years

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The PNPKI activates the cryptographic module containing its PNPKI CAs' private keys according to the specifications of the hardware manufacturer and the Key Ceremony Document. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. It can only be activated through the use of HSM smart cards (3 of 10) accomplished by strong passwords. All smart cards are stored in a safe when not in use. The cryptographic hardware is held under three-person control as explained in Section 5.2.2 (Number of Persons Required Per Task) and elsewhere in this CPS.

All PNPKI personnel are required to use strong passwords and to protect PINs and passwords. The PNPKI requires that passwords to workstations be changed on a regular basis.

6.4.2 Activation Data Protection

Activation data for HSM devices are protected as described in Section 6.2.2 (Private Key (n out of m) Multi-Person Control). PNPKI CA and RA are required to store their administrator private keys in encrypted form using hardware token with strong password protection.

The PNPKI recommends that subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

All computers able to access the PNPKI CA environment shall be protected by a combination of operating system, software and physical safeguards. All RAs that are accredited should comply with all the rules and guidelines stated in the accreditation.

6.5.1 Specific Computer Security Technical Requirements

The PNPKI ensures that the systems maintaining the PNPKI CA software and data files are secure from unauthorized access. All computers that are part of the PNPKI CA system shall be configured and hardened using industry best practices. All operating systems shall require identification and authentication for authenticated logins. It shall provide discretionary access control, access control restrictions to services based on authenticated identity, security audit capability and a protected audit record for shared resources, self-protection, and process isolation.

The PNPKI CAs production network is logically separated from other components. This separation prevents network access except through defined application processes. The PNPKI uses firewalls to protect the production network from external intrusion and limit the nature and source of network activities that may access production systems.

Direct access to the PNPKI CA databases supporting the PNPKI CA operations is limited to the database administrator duly authorized for such access.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

The PNPKI has mechanisms to control and monitor the security-related configurations of its PNPKI CA systems. Change control processes consist of change control data entries that are processed, logged and tracked for any security-related changes to PNPKI CA systems, firewalls, routers, software and other access controls. In this manner, the PNPKI can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management through accomplishment of an approved change request form.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The PNPKI system is protected by firewalls. The RootCA is offline and not reachable from the network. Firewalls and boundary control devices are configured to allow access only by the addresses, port, protocols and commands required for the provision of PKI services by such systems.

The PNPKI CA equipment is configured with minimum number of services and all unused network ports and services are disabled. All firewall configuration changes are documented, authorized, tested and implemented in accordance with change management policies and procedures. Network configuration is available for review by its auditors and consultants under an appropriate non-disclosure agreement.

6.8 Time-Stamping

All the PNPKI CAs employ time-stamping on all security related transactions using trusted time source in compliance with the Philippine Standard Time Act of 2013 (R.A. 10535).

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificate issued under this CPS shall conform to the RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.1.1 Version Number(s)

All CAs Certificates are X.509 version 3 certificates. Subscriber Certificates shall be X.509 v3.

7.1.2 Certificate Extensions

The PNPKI populates X.509 version 3 Certificates with the extensions that comply with RFC 5280.

7.1.2.1 Key Usage

X.509 version 3 Certificates are generally populated in accordance with RFC 5280. The Key Usage extension in X.509 version 3 Certificates are generally configured in accordance with the following table.

	CAs	Subscriber Authentication Certificate	Subscriber Signing Certificate	Subscriber SSL Certificate
Critical	False	False	False	False
Digital Signature	Clear	Set	Clear	Set
Non-Repudiation	Clear	Clear	Set	Clear
Key Encipherment	Clear	Set	Clear	Set
Data Encipherment	Clear	Clear	Clear	Clear
Email Protection	Clear	Set	Clear	Clear
Client Authentication	Clear	Set	Clear	Clear
Server Authentication	Clear	Clear	Clear	Set
Key Certificate Sign	Set	Clear	Clear	Clear
CRL Sign	Set	Clear	Clear	Clear

7.1.2.2 Certificate Policies Extension

The `certificate Policies` extension of X.509 version 3 Certificates are populated with the object identifier for the PNPKI CP in accordance with CPS section 7.1.6 (Certificate Policy Object Identifier) and with policy qualifiers set forth in CP Section 7.1.8 (Policy Qualifier Syntax and Semantics). The criticality field of this extension shall be set to FALSE.

7.1.2.3 Subject Alternative Names

The subjectAltName extension of X.509 version 3 Certificate are populated in accordance with RFC 822. The criticality field of this extension shall be set to FALSE.

7.1.2.4 Basic Constraints

X.509 version 3 PNPKI CA Certificates BasicConstraints extension shall have the PNPKI CA field set to TRUE. End-user Subscriber Certificates BasicConstraints extension, shall be populated with a value of an empty sequence. The criticality field of this extension shall be set to TRUE for PNPKI CA Certificates, but otherwise set to FALSE.

X.509 version 3 PNPKI CA Certificates shall have a "pathLenConstraint" field of the BasicConstraints extension set to the maximum number of PNPKI CA certificates that may follow this certificate in a certification path. The PNPKI CA issuing subscriber certificates shall have a "pathLenConstraint" field set to a value of "0" indicating that only a subscriber certificate may follow in the certification path.

7.1.2.5 Extended Key Usage

The PNPKI uses the ExtendedKeyUsage extension for the specific types of X.509 version 3 Certificates.

For these certificates, the PNPKI populates the ExtendedKeyUsage extension in accordance with the table below.

	CA Certificate	OCSP Signer Certificate	TSA Signer Certificate	Subscriber Authentica-tion Certificate	Subscriber Signing Certificate	Subscriber SSL Certificate
Criticality	False	False	False	False	False	False
Server Authentication	Clear	Clear	Clear	Clear	Clear	Set
Client Authentication	Clear	Clear	Clear	Set	Clear	Clear
Email Protection	Clear	Clear	Clear	Set	Clear	Clear
Time Stamping	Clear	Clear	Set	Clear	Clear	Clear
OCSP Signer	Clear	Set	Clear	Clear	Clear	Clear

7.1.2.6 CRL Distribution Points

Most X.509 version 3 Subscriber Certificates and PNPKI CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the PNPKI CA Certificate's status. The criticality of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

The PNPKI generally populates the Authority Key Identifier extension of X.509 Version 3 Subscriber Certificates and PNPKI CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the PNPKI CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Where the Issuing CA populates X.509 version Subscriber Certificates with a `subjectKeyIdentifier` extension, the `keyIdentifier` based on the public key of the subject of the certificate is generated in accordance with one of the methods described in RFC 3280. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.3 Algorithm Object Identifiers

Cryptographic algorithm object identifiers are populated according to the RFC 5280 standards and recommendations.

7.1.4 Name Forms

The PNPKI CAs name forms are stipulated in Section 3.1 (Naming) of this CPS and the Naming and Profile Document.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a Certificate Policy and/or Certification Practice Statement, such as this CPS. The CP OIDs that incorporate this CPS into a given certificate by reference are listed in Section 1.2 (Document Name and Identification).

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

The PNPKI CA supports X.509 version 2 CRLs and CRL Profile.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. The PNPKI operates an OCSP service at http://govca.npki.gov.ph/ocsp.

The PNPKI OCSP Responder conforms to RFC 2560.

8. Compliance Audit and Other Assessments

The Compliance audit is conducted annually to all PNPKI CAs operating under this CPS. An RA operating under this CP is required to perform regular self-audit in compliance with its contractual obligation with the PNPKI.

8.1 Frequency or Circumstances of Assessment

Once a year, all PNPKI CAs shall be subject to audit in respect with its accreditation as specified under Section 3(d)(3) of E.O. 810, s2009 and Section 4 of DTI DAO No. 10-09, s2010.

8.2 Identity/Qualifications of Assessor

The audit requirement shall be performed by a qualified independent assessment team organized by the DTI-PAO comprising, but not limited to, the following:

a) Certified Public Accountants; and
b) Certified Information Security practitioners.

All shall possess sufficient knowledge on digital signatures, digital certificates, Internet X.509 version 3 PKI Certificate Policy and Certification Practices Framework, the Electronic Commerce Act of 2000, the Data Privacy Act of 2012, the Cybercrime Prevention Act of 2012 and E.O. 810, s2009 among others.

Compliance audit shall be performed by an accounting firm, accredited with the SEC, and:

a) Has proficiency in security auditing, information security tools and techniques, PKI technology and third-party attestation functions;
b) Holds particular skill sets, competency testing, quality assurance measures like peer review, standards with respect to proper assignment of staff to engagements and requirements for continuing professional education.

8.3 Assessor's Relationship to Assessed Entity

Any member of the assessment team and the firms or companies the member is affiliated with shall have no conflict of interest with the PNPKI CA being assessed and shall not be a software or hardware vendor that is or has been providing services or supplying equipment to the PNPKI CA within the last two (2) years.

8.4 Topics Covered by Assessment

The scope of the assessment includes: key management operations, PNPKI CA environmental controls, certificate lifecycle management, PNPKI CA business practices disclosure and Infrastructure / Administrative PNPKI CA controls.

8.5 Actions Taken as a Result of Deficiency

The Office of the Executive Director of the ICT Office-NCC shall formulate a corrective action plan that shall be implemented to rectify any noted deficiency based from the inputs of the auditor.

8.6 Communications of Results

A copy of the assessment report shall be submitted to DTI-PAO within four (4) weeks after completion of an assessment. The assessment report will be submitted in conformance with Section 4.4.5 of DTI-DAO No. 10-09, s2010.

9. Other Business and Legal Matters

9.1 Fees

All PNPKI CAs or RAs operating under this CPS may charge fees for the issuance of certificates in compliance with Administrative Order No. 31, s2012.

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

The PNPKI may charge a fee for making a certificate available to its repository or making certificates available to relying parties.

9.1.3 Revocation or Status Information Access Fees

The PNPKI does not charge fees for revocation of a certificate or for a relying party to check the validity status of an issued certificate through the use of Certificate Revocation Lists. The PNPKI reserves the right to establish and charge a reasonable fee for providing certificate status information services via OCSP.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

All PNPKI CAs operating under this CPS shall be insured against liabilities for damages in accordance with the provision of Section 4.2.2 of DTI-DAO 10-09, s2010.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

Information about the PNPKI CA or RA not requiring protection or confidentiality shall be made publicly available for transparency purposes. The mode of access to such information shall be determined by each respective organization.

9.3.1 Scope of Confidential Information

The PNPKI keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel:

a) All PNPKI CAs private keys;
b) Any activation data used to access private keys or gain access to the PNPKI CA system;
c) Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information;
d) Any information held by the PNPKI CA system as private information in accordance with Section 9.4 (Privacy of Personal Information);
e) Any transactional, audit log and archive record identified in Section 5.4 (Audit Logging Procedures) or 5.5 (Records Archival) including certificate application records and documentation submitted in support of certificate applications whether successful or rejected; and
f) External or internal audit trail records and any audit reports (with the exception of an auditor’s letter confirming the effectiveness of the control set forth in this CPS).

9.3.2 Information Not Within the Scope of Confidential Information

Subscriber application data being published in a digital certificate is considered public and not within the scope of confidential information. Certificate revocation and other status information are not considered confidential/private information. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

The PNPKI observes applicable rules on the protection of personal data deemed by law or privacy policy (see Section 9.4 of this CPS) to be confidential.

9.4 Privacy of Personal Information

A PNPKI CA or RA shall keep all subscriber-specific information confidential except as required by law or pursuant to an order of court.

All PNPKI CAs complies with the requirements under Section 12.13 of DTI-DAO No. 10-09 on the confidentiality of subscriber-specific information except as required by law or pursuant to an order of court.

9.4.1 Privacy Plan

All PNPKI CAs and/or RAs have Privacy Plans that will always protect personally identifying information from unauthorized disclosure.

9.4.2 Information Treated as Private

Any information about subscribers that is not publicly available through the content of the issued certificate and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

Information appearing in the certificate and CRL is not considered private.

9.4.4 Responsibility to Protect Private Information

All PNPKI CAs and RAs shall secure all private information they receive from compromise and disclosure to unauthorized parties and shall comply with the Data Privacy Act of 2012.

9.4.5 Notice and Consent to Use Private Information

Any disclosure of subscriber-specific information by a PNPKI CA or RA shall comply with the requirements of R.A. 10173 and must be authorized by the subscriber or as required by law or court order.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

A PNPKI CA or RA shall not disclose any private information to any third party unless authorized by this CPS, required by law or a court order. Any request for release of information shall be processed according to an established procedure.

9.4.7 Other Information Disclosure Circumstances

All PNPKI CAs comply with the requirements of the Data Privacy Act of 2012 in the event of disclosure of personal information.

9.5 Intellectual Property Rights

The intellectual property rights held by individuals, organizations, or entities shall always be upheld by all PNPKI CAs or RAs operating under this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

A PNPKI CA will operate its certification and repository services, issue and revoke certificate and issue CRLs in accordance with the requirements of this CPS.

Identification and authentication procedures shall be implemented as specified in Section 3 (Identification and Authentication) of this CPS.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

Subscribers of a PNPKI CA operating under this CPS shall agree to the following:

a) Accurately represent themselves in all communications with the PKI authorities.
b) Their private keys are protected and that no unauthorized person has ever had access to their private key.
c) Promptly notify the appropriate PNPKI CA/RA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through procedures consistent with the PNPKI CA's CPS.
d) Abide by all the terms, conditions and restrictions on the use of their private keys and certificates.
e) For SSL Certificates, install the certificate only on the server accessible at the domain name listed on the certificate, and use the certificate solely in compliance with applicable laws, and in accordance with the End-User Subscriber Agreement.

9.6.4 Relying Party Representations and Warranties

A relying party accepts that to reasonably rely on a certificate, it must:

a) Make reasonable efforts to acquire sufficient knowledge on using digital certificates and PKI.
b) Study the limitations on the usage of digital certificates.
c) Verify the certificates by referring to the relevant CRL or OCSP available through the PNPKI.
d) Trust a certificate only if it is valid and has not been revoked or has expired.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

A PNPKI CA or RA assumes no liability except as stated in the relevant contracts pertaining to certificate issuance and management.

9.8 Limitations of Liability

A PNPKI CA or RA shall not be liable for any damages to subscribers, relying parties or any other parties arising out of or related to the misuse of, or reliance on certificate issued by a PNPKI CA that has been:

a) Revoked;
b) Expired;
c) Used for unauthorized purposes;
d) Tampered with;
e) Compromised; or
f) Subject to misrepresentation, misleading acts or omissions.

9.9 Indemnities

End-user subscribers and relying parties shall agree to indemnify and hold a PNPKI CA or RA free from any claims, actions or demands that are caused by the use or publication of a certificate and that arises from:

a) Any false or misleading statement of fact by the subscriber;
b) Any failure by the end-user subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive;
c) Any failure on the part of the end-user subscriber to protect its private key and/or token if applicable or to take the precautions necessary to prevent the compromise, disclosure, loss, modifications or unauthorized use of the subscriber's private key; or
d) Any failure on the part of the subscribe to promptly notify the PNPKI CA or RA of the compromise, disclosure, loss, modification or unauthorized use of the subscriber's private key once the subscriber has actual or constructive notice of such event.

9.10 Term and Termination

9.10.1 Term

This CPS becomes effective upon approval by the Executive Director of ICT Office-NCC and its publication in the PNPKI CA repository of documents in its website.

9.10.2 Termination

This CPS shall remain in force until it is amended or replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, PNPKI CAs are bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

The ICT Office-NCC, as Root CA, shall establish appropriate procedures for communications with PNPKI CA or RA through memorandum of understanding as applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

The ICT Office-NCC, as Root CA, shall review this CPS annually. Corrections, updates or suggested changes to this CPS shall be communicated to every PNPKI CA, designated or accredited. Such communication must include a description of the change, a change justification and contact information of the person requesting the change.

9.12.2 Notification Mechanism and Period

Proposed changes to this CPS shall be distributed electronically to PNPKI CAs and other bodies/entities formed to oversee the implementation of the National Certification Scheme for Digital Signatures in the Philippines. The notification shall contain the final date for receipt of comments and the proposed effective date of change.

9.12.3 Circumstances under Which OID Must Be Changed

If a change in CP or CPS is determined by the Policy Authority to warrant a change in the currently specified OID for a particular type of certificate, the revised version of this CPS will also contain a revised OID for that type of certificate.

9.13 Dispute Resolution Provisions

Any dispute arising from this CPS, or pertaining to the use and issuance of certificates issued under this CPS, shall be resolved amicably by ICT Office-NCC, through alternative dispute resolution between parties, subject to implementing guidelines to be issued.

9.14 Governing Law

The use and issuance of certificates under this CPS shall be covered by the applicable provisions of R.A. 8792 (the Electronic Commerce Act of 2000), R.A. 8484 (Access Devices Regulation Act of 1998), R.A. 7394 (the Consumer Act of the Philippines), R.A. 10173 (Data Privacy Act of 2012) and E.O. 810, s2009 (Framework for National Certification Scheme for Digital Signatures).

9.15 Compliance with Applicable Law

This CPS is subject to any applicable laws.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If any section of this CPS is determined to be incorrect or invalid, the other sections of this CP that are not affected shall remain in effect until the CP is updated. The process for updating this CP is described in Section 9.12 (Amendments) above.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The PNPKI accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as, but not limited to, the following:

a) Acts of God;
b) Acts of War;
c) Acts of Terrorism;
d) Epidemics;
e) Power or telecommunication services failure;
f) Earthquake;
g) Flood;
h) Fire; or
i) Any other natural or man-made disasters.

9.17 Other Provisions

No stipulation.

Appendix A
Acronyms and Abbreviations

ACA - Accredited Certification Authority

ARA - Accredited Registration Authority

BPS - Bureau of Product Standard

CA - Certification Authority

CP - Certificate Policy

CPS - Certification Practice Statement

CRL - Certificate Revocation List

DAO - Department Administrative Order

DN - Distinguished Name

DTI - Department of TRade and Industry

EAL - Evaluation Assurance Level

E.O. - Executive Order

FIPS - Federal Information Processing Standard

GovCA - Government Certification Authority

IETF - Internet Engineering Task Force

ISO - International Organization for Standardization

ICT Office-NCC - Information and Communications Technology Office - National Computer Center

LDAP - Lightweight Directory Access Protocol

OCSP - Online Certificate Status Protocol

OID - Object Identifier

PAO - Philippine Accreditation Office

PhilCA - Philippine Root Certification Authority (also the Root CA)

PKI - Public Key Infrastructure

PKIX - Public Key Infrastructure X.509 Working Group

R.A. - Republic Act

RA - Registration Authority

RFC - Request for Comment

URL - Uniform Resource Locator

Appendix B
Definitions

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).

Authentication - The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below.

Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

CA certificate - A certificate for one CA's public key issued by another CA.

Certificate Policy (CP) - A set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

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 certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Summary (or CPS Abstract) - A subset of the provisions of a complete CPS that is made public by a CA.

Identification - The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes:

(1) Establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization; and

(2) Establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing Certification Authority (Issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject Certification Authority). Chokhani, et al. Informational [Page 7] RFC 3647 Internet X.509 Public Key Infrastructure November 2003

Participant - An individual or organization that plays a role within a given PKI as a Subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS) - An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Policy Qualifier – Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Registration Authority (RA) - An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, 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 re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party - A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying Party Agreement (RPA) - An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Set of Provisions - A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework.

Subject Certification Authority (Subject CA) - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

Subscriber - A subject of a certificate who is issued a certificate.

Subscriber Agreement - An agreement between a CA and a Subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation - The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

Modification History

Version	Effective Date	Changes
1.0	December 23, 2013	