Philippine National Public Key Infrastructure (PKI)

Certificate Policy version 2.0

January 18, 2017

Version: 2.0
Effective: January 18, 2017

Philippine National PKI Certificate Policy

Content

Purpose

This policy shall serve as a guide to Certification Authorities (CAs). This is a set of rules governing the applicability of a certificate to a particular community and/or class of application with common security requirements.

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 computers.

Issuing Authority

This document has been compiled and issued by the Department of Information and Communications Technology (DICT) and DOST-Advance Science and Technology Institute (ASTI), through the Integrated Government Philippines (iGovPhil) Project.

Contact Information

Associated publications under iGovPhil Project can be found at http://i.gov.ph. Specific information related to the Philippine National PKI can be found at http://i.gov.ph/pnpki/.

Queries, suggestions, and clarifications with regard to this document may be forwarded to support.pnpki@dict.gov.ph.

1. Introduction

1.1 Overview

This Certificate Policy (hereafter referred as CP) applies to Certification Authorities issuing: (1) general purpose certificate, which can be used for all government and private transactions; and (2) specific purpose certificate, which can only be used for a specific transaction, issued by a Government Certification Authority (GovCA) or private Accredited Certification Authority (ACA).

A CP is a set of rules that defines the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP may define the 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.

This CP applies to certificates issued under the certification scheme for digital signatures as mandated by Executive Order No. 810, series of 2009 (EO810, s2009). This CP is applicable to GovCA and ACA.

This CP is consistent with Request for Comments 3647 (RFC3647) of the Internet Engineering Task Force (IETF) Internet X.509 version 3 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

The Certification Practice Statement (CPS) describes the manner in which the policy statements need to be executed. The CPS usually contains information regarding specific procedures that should be followed in compliance with the certificate policy.

For purposes of this policy, SSL certificates are considered general purpose certificates.

1.2 Document Name and Identification

This document is the PNPKI Certificate Policy. As detailed in this CP, 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 CP OID
Philippine Root CA	2.16.608.2.1.1.1
Philippine Government CA	2.16.608.2.2.1.1
Gov Authentication CA	2.16.608.2.3.1.1
Gov Signing CA	2.16.608.2.4.1.1
Gov SSL CA	2.16.608.2.5.1.1

1.3 PKI Participants

1.3.1 Certification Authority

a) Root Certification Authority (CA)

The PNPKI RootCA is the primary trust point for the entire PKI architecture. The National Computer Center (NCC), designated to operate a hierarchy of Philippine Certification Authorities, was abolished and all its powers and functions, applicable funds and appropriations, records, equipment, property and personnel were transferred to the DICT as per Section 15(a) of R.A. 10844.

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 RootCA and approved CA signing keys;
iv) Establishment and maintenance of the CPS;
v) Provide technical expertise in the conduct of assessment of 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 Certificate 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. Send 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 CA policies;
b) Issue and manage certificates for general or specific purpose to user or juridical entities;
c) Publish issued certificates and revocation information;
d) Handle revocation request regarding certificate issued by the CA; and
e) Send notification of issuance, revocation or renewal of certificates.

1.3.2 Registration Authority (RA)

The CA may designate specific RAs to perform the Subscriber Identification and Authentication, certificate request and revocation functions defined in the CP and related documents.

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

a) Identify the user and register the user information;
b) Transmit the certificate request to the CA;
c) Validate certificates from the 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 juridical entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the keys and certificate in accordance with the certificate policy, including the following:

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 if the private key is compromised.

1.3.4 Relying Parties

A relying party is the entity that relies on the validity of the binding of the subscriber’s name to a public key. The relying party is responsible for checking the status of 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) Purpose for which a 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

a) Accreditation and Assessment Body

E.O. 810, s2009 mandates the Department of Trade and Industry (DTI), through its Philippine Accreditation Bureau (PAB), as the accreditation and assessment body for Certification Authorities (CAs). DTI-PAB is responsible for the functions stipulated under Section 3(d) of EO810, s2009.

b) DTI-Bureau of Philippine Standards (DTI-BPS)

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

1.4 Certificate Usage

A subscriber agrees to use the certificate for its lawful and intended use 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 in the 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 CP;
b) The certificate is being used in accordance with its Key-Usage field extensions; and
c) The certificate is valid at the time of reliance by reference to OCSP or CRL.

1.4.2 Prohibited Certificate Usage

All certificates issued under this policy cannot be used for purposes other than what is allowed in Section 1.4.1 (Appropriate Certification Usage) above.

1.5 Policy Administration

1.5.1 Organization Administering This CP

The DICT is responsible for all aspects of this CP.

Philippine National PKI
DICT Building
Carlos P. Garcia Avenue
U.P. Campus, Diliman
1101 Quezon City, PHILIPPINES
Tel. No.: (+632) 920-0101
Fax No.: (+632) 426-1525

1.5.2 Contact Person

Office of the Secretary
DICT Building
Carlos P. Garcia Avenue
U.P. Campus, Diliman
1101 Quezon City, PHILIPPINES
EMail: support.pnpki@dict.gov.ph
Tel. No.: (+632) 920-0101
Fax No.: (+632) 426- 1525

1.5.3 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 CPS is one of the assessment requirements by the DTI-PAB.

Philippine Accreditation Bureau
3/F Trade and Industry Building
361 Sen. Gil J. Puyat Avenue
Makati City
EMail: pab@dti.gov.ph
Tel. No.: (+632) 751-4707
Fax No.: (+632) 751-3262

1.5.4 Approval Procedures

A PNPKI CA operating under this CP shall follow the CPS approval process issued by DTI-PAB 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.

2.2 Publication of Certification Information

All CAs that issue certificates under this CP shall post all CA certificates issued in a directory publicly accessible through the Lightweight Directory Access Protocol (LDAP) or Hypertext Transfer Protocol (HTTP). To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

Published certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the CA or other authorized parties.

2.3 Time or Frequency of Publication

A certificate shall be published in repositories as soon as it is issued, renewed or revoked.

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

2.4 Access Controls on Repositories

All CAs operating under this CP shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions, the restricted information may be made available.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

CAs operating under this CP shall only generate and sign certificates that contain a non-null subject Distinguished Name (DN).

Each CA must have a unique and readily identifiable Distinguished Name according to the X.500 standard. Details of naming conventions for CAs are found in their respective Certificate Profiles.

3.1.2 Need for Names to be Meaningful

Names used in the certificates must identify the name of the subscriber in a meaningful way to which they are assigned. The name used in the certificate is in a form commonly understood semantically in order to determine the identity of a person and/or organization. A name is meaningful only if the names that appear in the certificates can be understood and used by Relying Parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

CAs operating under this CP shall not issue anonymous certificates. Pseudonymous certificates may be issued under this CP 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 Philippine issuing CAs ensures the Subject DNs are unique within the domain of a specific CAs through automated components of the subscriber enrollment process. It is possible for a subscriber to have two or more certificates with the same Subject DNs.

3.1.6 Recognition, Authentication and Role of Trademarks

Subscribers may not request certificates with any content that infringes into the intellectual property rights of another entity.

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

3.2.2 Authentication of Organization Identity

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

Philippine 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 CA.

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

a) Tax Payer Identification Number (TIN);
b) Authorization Letter or Board Resolution naming the authorized representative/s to apply for a digital certificate in behalf of the agency;
c) Consent to verify and share 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 containing the 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 nongovernment 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 complied:

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 representative, the 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) Taxpayer 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 ID's 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-sized photo taken within the last six (6) months;
e) Phone number (mobile and/or landline);
f) Email address owned by the individual or authorized by the owner for use by the subscriber;
g) Latest copy of a bill containing the address of the applicant where the PIN, which will be used to activate a digital certificate, shall be mailed; and
h) Consent to verify and share the information submitted.

3.2.4 Non-Verified Subscriber Information

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

3.2.5 Validation of Authority

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

3.2.6 Criteria for Interoperation

The DICT, through PNPKI RootCA, shall allow inter-operation of a non-PNPKI CA in circumstances where the 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 Requests

3.3.1 Identification and Authentication for Routine Re-Key

CA certificate re-key shall follow the same procedure as that of initial key generation.

Subscriber certificates shall be subject for re-key on a case-to-case basis.

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.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated and comply with 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 with authority to make the revocation request;
b) Immediately upon revocation, publish a signed notice of the revocation or a Certificate Revocation List 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 date and time of all transactions in relation to the revocation request.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

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

4.1.1 Who Can Submit a Certificate Application

Only accredited CAs can submit a Certificate Application to be signed by PNPKI RootCA or Subordinate CAs in conformity with Section 3 (Identification and Authentication) above.

An individual applicant or authorized representative can submit a Certificate Application Form directly to an Issuing CA.

4.1.2 Enrolment Process and Responsibilities

The applicant shall be responsible for providing accurate information in the Certificate Application Form.

4.2 Certificate Application Processing

The information in Certificate Application Form must be verified 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 (Identification and Authentication) of this CP.

4.2.2 Approval or rejection of Certificate Application

The approval or rejection of certificate application is at the discretion of the CAs operating under this CP.

4.2.3 Time to Process Certificate Application

No stipulation.

4.3 Certificate Issuance

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

4.3.1 CA Actions during Certificate Issuance

The CA and/or RA shall verify the identity and authority (for juridical application) of a prospective subscriber before issuance of a certificate. The responsibility for verifying a prospective subscriber data shall be described in the CA's CPS. A certificate shall be checked to ensure that all fields and extensions are properly populated. After generation, verification and acceptance by the subscriber, the CA shall post the certificate in the repository system as specified in Section 2 (Publication and Repository Responsibilities) of this CP.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs/RAs operating under this CP may choose to inform the subscriber of the creation of their certificate and make the certificate available to the subscriber without reasonable delay.

4.4 Certificate Acceptance

Before a subscriber can use the private key, the CA/RA shall convey to the subscriber its responsibilities as defined in Section 9.6.3 (Subscriber Representations and Warranties) of this CP.

4.4.1 Conduct Constituting Certificate Acceptance

Failure to object to the certificate or its contents within five (5) calendar days, after notification of the issuance of the certificate constitutes

acceptance of the certificate. A subscriber agrees to the terms and conditions contained in this CP and the CPS of the CA.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2 (Publication and Repository Responsibilities) of this CP, 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 CA/RA operating under this CP may choose to notify other CAs or RAs of the certificate issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall protect their private keys from access by other parties at all times.

By using the certificate, a subscriber agrees to use the certificate for its lawful and intended use only.

4.5.2 Relying Party Public Key and Certificate Usage

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 CP.
b) That the certificate is being used in accordance with its Key-Usage field extensions; and
c) That the certificate is valid at the time of reliance by reference to OCSP or CRLs.

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.

4.6.1 Circumstance for Certificate Renewal

A 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.

4.6.2 Who May Request Renewal

A subscriber or authorized representative may request for renewal directly with the CA or through the RA.

4.6.3 Processing Certificate Renewal Requests

The CA or RA shall process requests for renewal by verifying that the subscriber information has not changed. The CA or RA shall estimate the validity time left of the keys considering the validity time of the new certificate.

4.6.4 Notification of New certificate Issuance to Subscriber

The notification of a renewed certificate to a subscriber follows the same routine as when a new certificate is issued as specified in Section 4.3.2 (Notification to Subscriber by the CA of Issuance of Certificate) of this CP. CAs/RAs operating under this CP may inform the subscriber of the issuance of renewed certificate as specified in Section 4.3.2 (Notification to Subscriber by the CA of Issuance of Certificate) of this CP.

4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

Failure to object to the certificate or its contents within five (5) calendar days, after notification of the renewal of the certificate, constitutes acceptance of the renewed certificate. A subscriber agrees to the terms and conditions contained in this CP and the CPS of the CA.

4.6.6 Publication of Renewed Certificate

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

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The CA/RA operating under this CP may choose to notify other CAs or RAs of the certificate issuance.

4.7 Certificate Re-key

4.7.1 Circumstance for Re-key

A certificate re-key may be done if it is deemed necessary due to one of the following reasons:

a) Migration of hardware;
b) The keys have low cryptographic strength;

c) The keys have high exposure; or
d) Enforced by a standard or application.

A re-key request is allowed only once in a year.

4.7.2 Who May Request for Re-Key

A request for re-keying may be done by a subscriber or the authorized representative of a juridical entity directly with the CA or RA. Section 3.3.1 (Identification and Authentication for Routine Re-key) of this CP shall be followed to verify the information of the subscriber.

4.7.3 Processing Certificate Re-Key Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

CA/RA operating under this CP 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 CP.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Failure to object to the certificate or its contents within five (5) calendar days, after notification of the re-keyed certificate, constitutes acceptance of the re-keyed certificate. A subscriber agrees to the terms and conditions contained in this CP and the CPS of the CA.

4.7.6 Publication of the Re-Keyed Certificate by the CA

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

4.7.7 Notification of Certificate Issuance to Other Entities

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

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Certificate modification is performed when change occurs in any of the information of an existing certificate. After modification, the original certificate may or may not be revoked but it must not be re-keyed, renewed or modified anymore.

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

Proof of all information changes must be provided to the CA or RA before the modified certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

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

A CA or RA may choose to notify other CAs or RAs of certificate issuances.

4.9 Certificate Revocation and Suspension

Any request for certificate revocation or suspension must be authenticated. A CA shall publish its CRL as specified in Section 2 (Publication and Repository Responsibilities) of this CP.

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer valid.

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

a) Key Compromise - The CA's private key has been compromised.
b) CA Compromise - The CA database has been compromised
c) The CA is determined to be not being compliant with its CP/CPS.
d) Cessation of Operation - The CA shall cease operation.

A CA issuing certificates to end-entities will revoke the end-entity's certificate if:

a) The CA determines that the subscriber is no longer meeting its policy requirement.
b) A CA or RA receives an authenticated request from an individual subscriber or an authorized representative of a juridical entity subscriber.
c) An authorized employee, named under Section 4.3.2 of DTI DAO No. 10-09, determines that an emergency specified under Section 12.12 of DTI DAO No. 10-09 has occurred that may impact the integrity of the certificates issued by the CA. Under this circumstance, the official performing the duty specified under Section 12.15.1 of DTI DAO No. 10-09 shall authorize the immediate revocation of the certificate.

4.9.2 Who Can Request Revocation

A request for certificate revocation may be done by the CA itself, a subscriber or the authorized representative of a juridical entity directly with the CA or RA.

4.9.3 Procedure for Revocation

The CA and/or RA shall verify the identity and authority (for juridical entity) of a subscriber making the request for revocation. The procedure for verifying the revocation request shall be described in the CA's CPS.

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

A revocation request shall be processed without delay.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties should validate any presented certificate against the most updated CRL or through OCSP.

4.9.7 CRL Issuance Frequency

a) Philippine RootCA shall publish its updated CRL at least once every three (3) months.
b) Subordinate CAs and Issuing CAs shall publish its CRL at least once every twenty four (24) hours.
c) Special purpose CAs shall publish their CRL based on the importance to provide correct status information.

The publication and frequency of CRL issuance shall be in conformance with Section 2 (Publication and Repository Responsibilities) of this CP.

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 On-Line Revocation / Status Checking Availability

CAs are to provide online validation service. If online validation is available, it is expected to perform revocation checks using the OCSP Server provided.

4.9.10 On-Line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

No stipulation.

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 Service

4.10.1 Operational Characteristics

Both OCSP and CRL are to be made available by a CA.

4.10.2 Service Availability

The certificate status validation service shall deliver 99.7% availability.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

No key escrow is delivered.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Management, Operational and Physical Controls

5.1 Physical Security Controls

All CA equipments, including cryptographic modules, shall be protected from unauthorized access at all times.

All the physical security control requirements specified below and any remote workstations used to administer the CA system, except where specifically noted, shall apply to all CAs.

5.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the 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 equipments and records of CAs.

5.1.2 Physical Access

The CA equipment, to include remote workstations used to administer the 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 to both the cryptographic module and computer systems; and
e) Ensure that all removable media and paper copies containing sensitive plain-text information are stored in secure containers.

5.1.3 Power and Air Conditioning

A 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 CA equipments shall be installed in a place where there is no 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 CA shall implement reasonable precautions against 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 CA's equipment. The backup shall be stored at a site with physical and procedural controls commensurate to the operational controls of the CA.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is a position assigned to a person who performs functions that require a high degree of trust. The person, however, can introduce security problems if the functions are not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA or RA is weakened. 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 positions are trusted roles:

Security Officer	Responsible for the overall administration and implementation of 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 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	Has privileged access to the database and can create users, databases and manipulate tables.

Administrator	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 the following tasks:

a) CA key generation
b) CA signing key activation
c) CA private key backup

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.

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.

5.2.4 Roles Requiring Separation of Duties

Role separation may be enforced either by the CA equipment, or procedurally, or by both means.

5.3 Personnel Security Controls

5.3.1 Background, Qualifications, Experience and Security 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 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 *("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 CA or RA shall receive comprehensive training in all operational duties they are expected to perform, including good knowledge on the following:

a) The 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 CA shall receive comprehensive training or demonstrate competence in the following areas:

a) CA/RA security principles and mechanisms;
b) All PKI software versions in use by the 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 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 CA's services.

5.3.6 Sanctions for Unauthorized Actions

Penalties shall be imposed on 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 CA or RA shall meet the personnel requirements set forth in this CP or the CA's CPS, as applicable.

5.3.8 Documentation Supplied to Personnel

For the 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 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 1009, series 2010.

5.4.1 Types of Events Recorded

A message from any source received by the CA requesting an action related to the operational state of the 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 the event occurred;
c) A success or failure indicator, where appropriate; and
d) The identity of the entity and/or operator (of the CA or RA) that caused the event.

The following are auditable events:

a) System Access
b) Physical Access
c) Key Generation
d) Certificate Lifecycle
e) Transaction Logs
f) System Logs
g) Application Logs

All security auditing capabilities of the CA's operating system and applications required by this CP shall be enabled. As a result, the events identified above shall be automatically recorded. Where events cannot be automatically recorded, the 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 CA audit log shall be retained as a minimum during its total life time.

Other audit logs shall be retained onsite until reviewed and remain for a period of ten (10) years from the date of issuance of the certificate.

5.4.4 Protection of Audit Log

The 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).

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 log 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 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 CP 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

Once a year, the CA shall assess the vulnerability of its CA system or its components. A routine assessment of the CA system shall be performed regularly for evidence of any malicious activity.

5.5 Records Archival

All CA or RA shall comply with their respective records retention policies in accordance with applicable laws and Section 12.2 of DTI DAO 1009, series 2010.

5.5.1 Types of Records Archived

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

a) Activities in issuance, renewal, suspension and revocation of certificates, including the process of identification of any person requesting a certificate from an accredited CA;
b) The process of generating subscribers' (where applicable) or the accredited CA's own key pairs; and
c) Such related activity of an accredited 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 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 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 CA operating under this CP 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

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 (RA 10535).

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedure to Obtain and Verify Archive Information

The procedures detailing how to create, verify, package, transmit and store archive information shall be published in the CPS of the CA.

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

5.6 Key Changeover

To minimize the risk from compromise of a CA's private signing key, the key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, public key will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that cover certificates signed with that key, then the old key must be retained and protected.

Key changeover procedures will establish key rollover certificates where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

CAs operating under this CP either must establish key rollover certificates as described above or must obtain a new CA certificate for the new public key from the issuers of their current certificates.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

A CA shall provide notice to DICT, as RootCA, and DTI-PAB of any incident falling within the following requirements:

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

If any of the incidents mentioned above happens, the accredited CA shall

report it to DICT, as RootCA, and DTI-PAB within the next working day.

5.7.2 Computing Resources, Software and/or Data are Corrupted

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

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

a) If the CA signature keys are compromised or lost (such that compromise is possible even though not certain):

   i. The RootCA and all of its member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA;
   ii. A new key pair shall be generated by the CA in accordance with procedures set forth in its CPS; and
   iii. New certificates shall be issued to subscribers also in accordance with the CA's CPS.

b) If the 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 CP.

c) The CA governing body shall also investigate and report to the DICT and DTI-PAB 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 CA directory system shall be deployed so as to provide 24 hour, 365 days per year availability.

The CA shall operate a backup site that will ensure continuity of operations in the event of failure of the primary site. The CA operations shall be designed to restore full service within six (6) hours of primary system failure.

5.8 CA or RA Termination

In the event that a CA terminates its operation, it shall provide notice to DICT, as RootCA, and DTI-PAB prior to termination in compliance with the requirements of Section 17.2 of DTI DAO 10-09, series 2010.

6. Technical Security Controls

The CA private keys are protected within a hardware security module (HSM) that meets 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

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.

All 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.

Generation of subscriber key pairs is generally performed by the Subscriber.

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 CA or RA generates keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or on a hardware cryptographic module. 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 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.

A 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

When key pairs are generated by the subscriber, the public key and the subscriber's identity must be delivered securely to a CA or RA for certificate issuance.

6.1.4 CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, it shall distribute the new public key in a secure fashion.

6.1.5 Key Sizes

CAs that generate certificates and CRLs under this CP shall use SHA-1, SHA224, SHA-256, SHA-384 or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued after 31 December 2030 shall be generated using, at a minimum, SHA256.

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)

Keys may be used for the purposes and in the manner described in Section 7.1 (Certificate Profile) of this CP.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

All CAs are required to take all appropriate and adequate steps in accordance with the requirements of this CP to protect and prevent the loss, damage, disclosure, modification or unauthorized use of their private keys.

6.2.1 Cryptographic Module Standards And Controls

The HSM used by a CA is required to meet at least level 3 of FIPS 140-2 in both the generation and maintenance of private keys.

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

All CA private keys shall be accessed through multi-person control as specified in Section 5.2.2 (Number of Persons Required Per Task) of this CP.

6.2.3 Private Key Escrow

Private keys shall not be escrowed.

6.2.4 Private Key Backup

The private keys of CAs are stored in encrypted state and access is only by multi-person control as specified in Section 6.2.2 (Private Key (n out of m) Multi-Person Control) of this CP. The private keys are backed up under further encryption and maintained on-site and in secure off-site storage.

For the backup of Subscriber private keys, subscribers may choose to backup their keys to their hard drive.

6.2.5 Private Key Archival

Private keys used for encryption shall not be archived.

6.2.6 Private Key Transfer Into or From A Cryptographic Module

If a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport.

6.2.7 Private Key Storage on Cryptographic Module

Private keys held in a cryptographic module are stored in an encrypted form and password-protected.

6.2.8 Method of Activating Private Key

CA signing activation requires multiparty control as specified in Section 5.2.2 (Number of Persons Required Per Task) of this CP.

6.2.9 Method of Deactivating Private Key

Private keys are deactivated by removing the token/key card from the reader, powering off the hardware cryptographic module, logging-off the application, automatic deactivation after use of the private key or time expiration.

6.2.10 Method of Destroying Private Key

A private key shall be destroyed by token surrender, token destruction, deletion or overwriting the key.

6.2.11 Cryptographic Module Rating

See Section 6.2.1 (Cryptographic Module Standards and Controls) of this CP.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival in accordance with Section 5.5 (Records Archival) of this CP.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period for the certificate of PNPKI RootCA shall be twenty-five (25) years while the maximum validity period for the certificate of GovCA shall be twenty-three (23) years. The validity period for the certificates for all issuing CAs shall not be more than eleven (11) years. A CA shall not issue a certificate that extends beyond the expiration date of its own certificate and public key. A subscriber's certificate shall have a maximum validity period of two (2) years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CAs and RAs shall generate their activation data for their private keys in accordance with the Key Ceremony Procedure.

Subscribers shall generate passwords that cannot be easily guessed or cracked by dictionary attacks through the Self-service portal.

6.4.2 Activation Data Protection

Data used to unlock a private key shall be protected from disclosure. Activation data shall be memorized, biometric in nature or recorded and secured at the level of assurance associated with the activation of the cryptographic module.

Activation Data Protection for CAs shall be in accordance with Key Ceremony Procedure.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

An RA shall follow the rules and guidelines issued by its corresponding CA for the information security requirements.

6.5.1 Specific Computer Security Technical Requirements

A CA shall have a formal Information Security Policy that documents the policies, standards and guidelines relating to information security. The computer security functions listed below are required. These functions may be provided by the operating system or through a combination of operating system, software and physical safeguards.

a) Require authenticated logins
b) Provide discretionary access control
c) Provide a security audit capability
d) Restrict access control to CA services and PKI roles
e) Enforce separation of duties for PKI roles
f) Require identification and authentication of PKI roles and associated identities
g) Archive audit data
h) Require self-test security related services
i) Require recovery mechanisms for keys and the CA system

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

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

All access to CA equipment via network shall be protected by network firewall and filtering router.

6.8 Time-Stamping

No stipulation.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificates issued under this policy shall conform to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.1.1 Version Number(s)

CAs shall issue X.509 v3 certificates.

7.1.2 Certificate Extensions

CAs shall use standard certificate extensions that comply with RFC 5280.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the Joint-ISO-ITU Object Identifier (OID).

7.1.4 Name Forms

The subject and issuer fields of the base certificate shall be populated with a nonempty X.500 Distinguished Name as specified in Section 3.1.1 (Types of Names) above. Distinguished names shall be composed of standard attribute types, such as those identified in RFC 5280.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP shall use the Joint-ISO-ITU OID number that points to the correct CA as well as Certificate Policy.

7.1.7 Usage of Policy Constraints Extension

The CA may assert policy constraints in CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP may contain policy qualifiers identified in RFC 5280.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

CAs operating under this CP shall issue X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

CAs operating under this CP shall use RFC 5280 CRL and CRL entry extension.

7.3 OCSP Profile

7.3.1 Version Number(s)

No stipulation

7.3.2 OCSP Extensions

No stipulation

8. Compliance Audit and Other Assessments

An RA operating under this CP is required to perform regular self-audit in compliance with its contractual obligation with the GovCA or ACA.

8.1 Frequency or Circumstances of Assessment

At least once a year, all 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-PAB 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 v3 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, registered 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 CA being assessed and shall not be a software or hardware vendor that is or has been providing services or supplying equipment to the CA within the last two (2) years.

8.4 Topics Covered By Assessment

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

8.5 Actions Taken As A Result Of Deficiency

The DICT shall formulate a corrective action plan that shall be implemented to rectify any noted deficiency based from the inputs of the auditor.

8.6 Communication of Results

A copy of the assessment report shall be submitted to DTI-PAB within four (4) weeks after completion of an assessment.

9. Other Business and Legal Matters

9.1 Fees

A CA or RA, whether government or private, operating under this CP shall be allowed to charge fees for the issuance of certificates in accordance with the requirements of Section 7 of E.O. 810, s2009.

Government agencies and instrumentalities performing the functions enumerated in Section 3 of E.O. 810, s2009 are required to comply with the provisions of Administrative Order No. 31, s2012.

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

Under Section 3(b)(2) of E.O. 810, s2009, the CA is required to publish certificates and the CRL. Thus, no additional fees for access to this information shall be made by the CA.

9.1.3 Revocation or Status Information Access Fees

A CA operating under this CP shall not charge any additional fees for accessing CRLs. Other revocation or status information may be charged for based on agreements with third parties.

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

A CA operating under this CP 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 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

No stipulation.

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

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

9.4.1 Privacy Plan

A CA or RA shall have a Privacy Plan to always protect personally identifying information from unauthorized disclosure.

9.4.2 Information Treated As Private

A CA or RA shall protect all personally identifying information of subscribers from unauthorized disclosure. A record of an individual transaction may be released upon request of the subscriber involved in the transaction. Any record from the archive maintained by a CA operating under this CP shall not be released except as required by law or a court order.

9.4.3 Information Not Deemed Private

Information included in Section 7 (Certificate, CRL and OCSP Profiles) of this CP is not subject to protection outlined in Section 9.4.2 (Information Treated as Public) above.

9.4.4 Responsibility to Protect Private Information

Confidential information must be stored securely and may be released only in accordance with the requirements of R.A. 10173.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant To Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

A CA or RA shall 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 an individual, organization or entities shall always be upheld by a CA or RA.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

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

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

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

a) Accurately represent themselves in all communications with the PNPKI authorities.
b) Protect their private keys at all times, in accordance with this CP.
c) Promptly notify the appropriate 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 CA's CPS.
d) Abide by all the terms, conditions and restrictions on the use of their private keys and certificates.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties Of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

A 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 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 certificates issued by a 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

Subscribers and relying parties shall agree to indemnify and hold a CA or RA harmless 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 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 subscriber to protect its private key and/or token if applicable or to take the precautions necessary to prevent the compromise, disclosure, loss, modification or unauthorized use of the subscriber's private key; or
d) Any failure on the part of the subscriber to promptly notify the 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 CP becomes effective upon approval by the Secretary of the DICT and its publication in the PNPKI Repository of documents in its website.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

The requirements of this CP shall remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

The DICT, as RootCA, shall establish appropriate procedures for communications with CA or RA through memorandum of understanding as applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

The DICT, as RootCA, shall review this CP at least once a year. Corrections, updates or suggested changes to this CP shall be communicated to every 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 CP shall be distributed electronically to 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

The Object Identifier of this CP shall not be changed unless the PNPKI RootCA determines that the issuance of a new certificate policy requires it to be so.

9.13 Dispute Resolution Provisions

Any dispute arising with respect to this CP, or pertaining to the use and issuance of certificates, issued under this CP, shall be resolved amicably by DICT, 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 CP 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

A CA or RA is required to comply with 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 CP 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 Philippine RootCA or any CA or RA 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 manmade disasters.

9.17 Other Provisions

No stipulation.

Appendix A

Acronyms and Abbreviations

ACA – Accredited Certification Authority

ARA – Accredited Registration Authority

CA – Certification Authority

CP – Certificate Policy

CPS – Certification Practice Statement

CRL – Certificate Revocation List

DAO – Department Administrative Order

DTI – Department of Trade and Industry

E.O. – Executive Order

GovCA – Government Certification Authority

IETF – Internet Engineering Task Force

ISO – International Organization for Standardization

DICT – Department of Information and Communications Technology

OID – Object Identifier

PAO – Philippine Accreditation Bureau

PhilCA – Philippine Root Certification Authority (also the RootCA)

PKI – Public Key Infrastructure

PKIX – Public Key Infrastructure X.509 Working Group

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 named 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 rekeying 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	Created RootCA-CP version 1.0
2.0	January 18, 2017	Amendment of RootCA-CP version 1.0 to reflect the change from NCC-ICTO to the Department of Information and Communications Technology (DICT) as the Philippine RootCA operator, renaming of DTI-PAO to DTI-PAB and the use of new OID mapping table for DICT.