# Philippine Navy
# Public Key Infrastructure (PN PKI)

## Certificate and Smart Card Policy version 1.0

30 April 2021

Philippine Navy PKI Certificate and Smart Card Policy

## Table of 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 the Philippine Navy.

## Scope

This document applies to PN Certification Authority that issues the following:

1. General purpose certificate, which can be used for all PN 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.

# 1. Introduction

## 1.1 Overview

This Certificate and Smart Card Policy applies to Certification Authorities issuing: (1) general purpose certificate, which can be used for all PN 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.

This provides a set of rules that defines the applicability of a certificate to PN electronic transactions such as but not Digital Signature, Client Logon, Server Authentication, IPMS, Logistics MIS, etc. This policy applies to certificates issued under the certification scheme for digital signatures as mandated by Executive Order No. 810, series of 2009 (EO810, s2009).

This policy 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.

This document is the PN PKI Certificate and Smart Card Policy. The PN PKI has the following issuers of digital certificates. The types of digital certificates issued are identified by the following object identifiers (OIDs):

| Certification Authority | PN PKI CP OID |
|---|---|
| PN Root CA | 2.16.608.2.1.1.1 |
| PN Issuing CA | 2.16.608.2.2.1.1 |
| PN Authentication CA | 2.16.608.2.3.1.1 |
| PN Signing CA | 2.16.608.2.4.1.1 |
| PN SSL CA | 2.16.608.2.5.1.1 |

## 1.2 Certification Authority

a) Root Certification Authority (CA)

The PN PKI RootCA is the primary trust point for the entire PKI architecture. The NICTC is designated to operate a hierarchy of PN Certification Authorities. The following are obligations of PN PKI RootCA:

i. Operate and manage the PNPKI RootCA system and its functions;
ii. Issue and manage Subordinate CA certificates;

iii. Re-key of the RootCA and approved CA signing keys

iv. Send notification of issuance, revocation or renewal of its certificates.

b) Subordinate Certification Authorities

The subordinate CAs include the Issuing CA, Authentication CA, PN Signing CA, SSL CA of the PN PKI. The following are obligations of the Subordinate CAs:

i. Operate and manage the subordinate CA system and its functions in accordance with the RootCA policy statement;

ii. Issue and manage certificates for Issuing CAs; and

iii. Send notification of issuance, revocation or renewal of its certificates.

The following are obligations of Issuing CA:

i. Operate and manage the issuing CA system and its functions in accordance to all applicable CA policies;

ii. Issue and manage certificates for general or specific purpose to user or juridical entities;

iii. Publish issued certificates and revocation information;

iv. Handle revocation request regarding certificate issued by the CA; and

v. Send notification of issuance, revocation or renewal of certificates.

### 1.3 Registration Authority (RA)

The CA may designate specific RAs to perform user identification and authentication, certificate request, and revocation functions defined in this document. 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.

For the purpose of this policy, all NICT Stations are hereby designated as RA within their area of responsibility.

### 1.4 Subscribers

A subscriber is any PN Personnel 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.

# 2. Certificate and Smart Card Application

## 2.1 Enrolment Process and Responsibilities

An application for a certificate shall be made directly with a CA operating under this policy and fulfilling the application requirements as enumerated in Section 2.2.1 (Identification and Authentication) of this document. PN Personnel or authorized representative can apply for PKI user certificate and Smart card through submission of duly accomplished Certificate Application Form (Annex A) directly to the RA (NICT Stations). The applicant shall be responsible for providing accurate information in the Certificate Application Form.

## 2.2 Certificate Application Processing

The information in Certificate Application Form must be verified before a certificate is issued.

### 2.2.1 Performing Identification and Authentication Functions

In all cases the applicant shall provide proof of identity such as Military or Government ID to the RA when applying for PKI certificate and Smart Card.

In the case of Certificate Signing Request (CSR), the applicant shall be required to prove possession of the private key that corresponds to the public key in the certificate request. In creating CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a distinguished name in the case of an X.509 certificate) which must be signed using the applicant's private key.

The Registration Authority (RA) shall verify the information contained in the Certificate Application Form.

.

### 2.2.2 Approval or Rejection of Certificate Application

The approval or rejection of certificate application is at the discretion of the RAs operating under this Policy.

### 2.2.3 Time to Process Certificate Application

Processing of certificate application shall be made within five (5) working days.

# 3. Certificate and Smart Card Issuance

## 3.1 Notification to Personnel on the Issuance of Certificate

The CA and/or RA shall verify the identity and authority of a prospective subscriber before issuance of a certificate. 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 notify the subscriber of the availability of his/her certificates and/or Smart Card.

In the case of renewal, re-keying, and modification of certificates stored in the Smart Card, the subscriber must hand over the card for re-writing/ re-encoding.

## 3.2 Certificate Acceptance

Before a subscriber can use the private key, the CA/RA shall convey to the subscriber its responsibilities as defined in Section 3.3 of this Policy. Failure to object to the contents of Certificate Usage 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 document.

## 3.3 Certificate Usage

A subscriber agrees to use the certificate and/or Smart Card for its lawful and intended use only.

### 3.3.1 Appropriate Certificate Usage

a) The PN PKI RootCA certificate can only be used for signing its CRL and the certificates of the subordinate CAs.

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 Issuing CAs can only be used strictly as part of the framework of the limitations incorporated in the certificates.

The subscribers, at the 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 Policy;

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.

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

### 3.3.2 Prohibited Certificate Usage

All certificates issued under this policy cannot be used for purposes other than what is allowed in Appropriate Certification Usage as specified in this document.

## 4. Certificate and Smart Card Renewal

### 4.1 Processing Certificate Renewal Requests

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. 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.

A subscriber or authorized representative may request for renewal directly with the CA or RA through submission of duly accomplished Certificate Renewal Form (Annex B).

### 4.2 Notification of Renewed Certificate Issuance to Personnel

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.

The notification of a renewed certificate to a subscriber follows the same routine as when a new certificate is issued as specified in this Policy.

### 4.3 Conduct Constituting Acceptance of a Renewed Certificate

The CA/RA shall convey to the subscriber its responsibilities as defined in Section 3.3 of this Policy. Failure to object to the contents of Certificate Usage 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 document

## 5. Certificate Modification and Re-keying

### 5.1 Processing Certificate Re-Key or Modification Requests

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.

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.

A subscriber or authorized representative may request for re-key or modification directly with the CA or RA through submission of duly accomplished Certificate Re-Key/ Modification Form (Annex C).

### 5.2 Notification of Re-keyed/ Modified Certificate Issuance to Personnel

The CA or RA shall process requests for re-keying or modification by verifying the subscriber information. The CA or RA shall estimate the validity time left of the keys considering the validity time of the new certificate.

The notification of a re-keyed/ modified certificate to a subscriber follows the same routine as when a new certificate is issued as specified in this Policy.

### 5.3 Conduct Constituting Acceptance of a Re-keyed or Modified Certificate

The CA/RA shall convey to the subscriber its responsibilities as defined in Section 3.3 of this Policy. Failure to object to the contents of Certificate Usage 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 document

# 6. Certificate Revocation and Suspension

## 6.1 Circumstances for Revocation and Suspension

A certificate shall be revoked when the private key of the subscriber has been compromised; or the binding between the subject and the subject's public key defined within a certificate is no longer valid.

The CA or the RA shall have the discretion to revoke or suspend the subscriber's certificate if any of the following condition transpires:

a) The CA determines that the subscriber is no longer meeting its policy requirement;

b) The CA or RA receives an authenticated request from an individual subscriber or an authorized representative of a juridical entity subscriber;

c) A competent authority determines that an emergency has occurred that may impact the integrity of the certificates issued by the CA. Under this circumstance, the CA shall authorize the immediate revocation of the certificate.

## 6.2 Procedure for Revocation and Suspension

### 6.2.1 Processing Certificate Revocation or Suspension Request

A request for certificate revocation or suspension may be done by the CA itself, the subscriber or authorized representative of a juridical entity directly with the CA or RA. The subscriber or authorized representative shall submit duly accomplished Certificate Revocation and Suspension Request Form (Annex D) to the RA or CA. Revocation request shall be processed without delay.

### 6.2.2 Validation of Revocation or Suspension Request

Any request for certificate revocation or suspension must be validated by the RA. Validated request shall be forwarded to the CA for re-generation and re-publishing of CRL.

### 6.2.3 Notification on the Result of Revocation or Suspension Request

The subscriber shall be notified on the status of the Certificate Revocation or Suspension within five (5) days from the request.

## 6.3 CRL Publication and OCSP Online Validation

The CA shall publish its updated CRL based on the following condition:

a) At least once every three (3) months;
b) Importance to provide correct status information; or
c) As soon as the request for revocation or suspension is approved.

The publication of CRL shall be done without any delay within four (4) hours of generation.

The CA shall provide online validation service. If online validation is available, it is expected to perform revocation checks using the OCSP Server provided. Both OCSP and CRL are to be made available by the CA.

# 7. Lost, Stolen, or Damaged Smart Card

## 7.1 Reporting of Lost, Stolen, or Damaged Smart Card

Lost, stolen, or damaged Smart Card must be reported to the RA or CA within 48 hours from the time of incident; and shall request for the revocation of certificate by accomplishing the Certificate Revocation and Suspension Request Form (Annex D). The subscriber must provide notarized affidavit of loss to the RA or CA for validation of the request.

The validation of lost, stolen, or damaged Smart Card follows the same routine as with the validation of Certificate Revocation/Suspension request as specified in this document.

Failure to report lost or stolen Smart Card within the allowed time shall be regarded as a cause for disciplinary action and a ground for non-issuance of another smart card.

## 7.2 Re-issuance of Smart Card

Re-issuance of Smart Card follows the same routine as when applying for new Certificate and/or Smart Card as specified in the above section of this document.

# 8. Certificate, CRL and OCSP Profiles

## 8.1 Certificate Profile

Certificates issued under this policy shall conform to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Distinguished names shall be composed of standard attribute types, such as those identified in RFC 5280.

### 8.1.1 Version Number(s)

The CA shall issue X.509 v3 certificates.

### 8.1.2 Certificate Extensions

The CA shall use standard certificate extensions that comply with RFC 5280.

### 8.1.3 Algorithm Object Identifiers and Name Forms

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

### 8.1.4 Certificate Policy Object Identifier

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

### 8.1.5 Usage of Policy Constraints Extension

The CA may assert policy constraints in CA certificates.

### 8.1.6 Policy Qualifiers Syntax and Semantics

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

## 8.2 CRL Profile

### 8.2.1 Version Number(s)

The CA shall issue X.509 version 2 CRLs

### 8.2.2 CRL and CRL Entry Extensions

The CA shall use RFC 5280 CRL and CRL entry extension.

## 9.1 Procedural Controls

### 9.2 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.

### 9.3 Records Archival

The CA shall comply with the records retention policies and in accordance with applicable laws of the Government. The minimum retention periods for archive data shall be ten (10) years.

### 9.4 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.

The CA shall 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.

### 9.5 Compromise and Disaster Recovery

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.

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.

## 9.6 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.

### 9.6.1 Key-pair Generation, Installation, and Private Key Protection

The CA key pair generation is performed by multiple pre-selected, trained and trusted Personnel 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. However, if the 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.

The CA is required to take all appropriate and adequate steps to protect and prevent the loss, damage, disclosure, modification or unauthorized use of their private keys.

### 9.6.2 Activation Data

The CA and RAs shall generate their activation data for their private keys. 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.

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

### 9.6.3 Computer Security Controls

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

### 9.6.4 Network Security Controls

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

## 9.7 Physical Security Controls

All CA equipment, including cryptographic modules, and remote workstations used to administer the CA systems shall be protected from unauthorized access at all times. 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.

## 9.8 Personnel Security Controls

Technical Personnel filling trusted roles shall be selected on the basis of loyalty, trustworthiness and integrity. All trusted roles are required to present proof of the requisite background, qualifications as well as experience necessary to efficiently and sufficiently perform their job responsibilities.

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

## 9.9 Compliance Audit and Legal Matters

At least once a year, the CA and RAs shall be subject to audit in respect with its accreditation and obligation as stipulated in this Policy. The audit requirement shall be performed by a qualified independent assessment team.

The 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.

### 9.9.1 Governing Laws

The use and issuance of certificates under this Policy 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).