Philippine National Public Key Infrastructure (PNPKI)

Time-Stamping Authority - Time-Stamp Policy / Practice Statement (PNPKI TSA-TSP / PS)

August 8, 2014

Version: 1.0
Effective: August 8, 2014
Object Identification Number: 2.16.608.1.20.1.1

Philippine National Public Key Infrastructure Time-Stamping Authority - Time-Stamp Policy / Practice Statement (PNPKI TSA-TSP/PS)

Contents

INTRODUCTION....4
1. SCOPE....4
2. REFERENCES....5
3. DEFINITIONS AND ABBREVIATIONS....5
3.1 DEFINITIONS....5
3.2 ABBREVIATIONS....6
4. GENERAL CONCEPTS....6
4.1 TIME-STAMPING SERVICES....6
4.2 TIME-STAMPING AUTHORITY....7
4.3 SUBSCRIBER....7
4.4 TIME-STAMP POLICY AND TSA PRACTICE STATEMENT....7
4.4.1 PURPOSE....7
4.4.2 LEVEL OF SPECIFICITY....8
4.4.3 APPROACH....8
5. TIME-STAMP POLICIES....8
5.1 OVERVIEW....8
5.2 IDENTIFICATION....8
5.3 USER COMMUNITY AND APPLICABILITY....8
5.4 CONFORMANCE....9
6. OBLIGATIONS AND LIABILITY....9
6.1 TSA OBLIGATIONS....9
6.1.1 GENERAL....9
6.1.2 TSA OBLIGATIONS TOWARDS SUBSCRIBERS....9
6.2 SUBSCRIBER OBLIGATIONS....10
6.3 RELYING PARTY OBLIGATIONS....10
6.4 LIABILITY....10
7. REQUIREMENTS ON TSA PRACTICES....10

7.1 PRACTICE AND DISCLOSURE STATEMENTS....11
7.1.1 TSA PRACTICE STATEMENT....11
7.1.2 TSA DISCLOSURE STATEMENT....11
7.2 KEY MANAGEMENT LIFE CYCLE....12
7.2.1 TSA KEY GENERATION....12
7.2.2 TSU PRIVATE KEY PROTECTION....12
7.2.3 TSU PUBLIC KEY DISTRIBUTION....13
7.2.4 REKEYING TSU'S KEY....13
7.2.5 END OF TSU KEY LIFE CYCLE....13
7.2.6 LIFE CYCLE MANAGEMENT OF THE CRYPTOGRAPHIC MODULE USED TO SIGN TIME-STAMPS....13
7.3 TIME-STAMPING....13
7.3.1 TIME-STAMP TOKEN....13
7.3.2 CLOCK SYNCHRONIZATION....14
7.4 TSA MANAGEMENT AND OPERATION....14
7.4.1 SECURITY MANAGEMENT....14
7.4.2 ASSET CLASSIFICATION AND MANAGEMENT....15
7.4.3 PERSONNEL SECURITY....15
7.4.4 PHYSICAL AND ENVIRONMENTAL SECURITY....15
7.4.5 OPERATIONS MANAGEMENT....15
7.4.6 SYSTEM ACCESS MANAGEMENT....16
7.4.7 TRUSTWORTHY SYSTEMS DEPLOYMENT AND MAINTENANCE....16
7.4.8 COMPROMISE OF TSA SERVICES....16
7.4.9 TSA TERMINATION....16
7.4.10 COMPLIANCE WITH LEGAL REQUIREMENTS....16
7.4.11 RECORDING OF INFORMATION CONCERNING OPERATION OF TIME-STAMPING SERVICES....16
7.5 ORGANIZATIONAL....17
8. CERTIFICATE PROFILE....17

Introduction

A digital signature is an online process that indicates approval to a particular datum presented in an electronic format, guaranteeing confidentiality and non-repudiation.

This digital signature ensures security, integrity, and reliability in the signed document. An electronically signed document is considered trusted digital evidence in that a tamper-resistant cryptographic seal is created around the electronic record.

The digital signature declares who signed a particular document. The person who signed the document is not able to revoke or deny the terms presented in it. An electronically signed document cannot be changed during or upon the signing event.

It is essential to couple the time of signing to the electronic document using a digital signature.

The time-stamp ensures time validity of an electronically signed document. Using a time-stamp, issued by a trusted Time-Stamping Authority (TSA), guarantees that a particular process occurred at a particular time and a certain datum existed at a certain point in time. Likewise, this guarantees that the person who signed the document cannot backdate the time stamp on the signature block.

1. Scope

This document, the Philippine National Public Key Infrastructure Time-Stamping Authority-Time-Stamp Policy / Practice Statement (PNPKI TSA-TSP/PS), which addresses the Time-Stamping Services (TSSs), describes the operational and management policy / practices to which the Philippine TSA follows.

Specifically, the PNPKI TSA-TSP/PS defines the following:

a) General policies and practices to be employed by the PNPKI TSA for issuing Time-Stamp Tokens (TSTs); and
b) Parties involved (PNPKI TSA, Subscriber, Relying Party), obligations, rights, and the applicability range.

Specific information related to the PNPKI, particularly to the PNPKI TSA's Time-Stamping Service, can be found at http://i.gov.ph/pki/.

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

2. References

Documents relevant to this document are as follows:

a) RFC 3161: IETF RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) – August 2001
b) RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs)
c) PNPKI Certificate Policy – December 23, 2013
d) PNPKI Certification Practice Statement – December 23, 2013

3. Definitions and Abbreviations

3.1 Definitions

Term	Description
Relying Party	Recipient of a time-stamp token who relies .on that time-stamp token
Subscriber	Entity requiring the services provided by a TSA and which has explicitly or implicitly .agreed to its terms and conditions
Time-Stamp Token	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that .time
Time-Stamping Authority	.Authority which issues time-stamp tokens
TSA Disclosure Statement	Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet .regulatory requirements
TSA Practice Statement	Statement of the practices that a TSA .employs in issuing time-stamp tokens
TSA System	Composition of IT products and components organized to support the provision of .time-stamping services
Time-Stamp Policy	Named set of rules that indicates the applicability of a time-stamp token to a particular community and / or class of application with common security

	.requirements
Time-Stamping Unit	Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a .time
Coordinated Universal Time	Time scale based on the second as defined in .(ITU-R Recommendation TF.460-5 (TF.460-5

Other terms are defined in the Memorandum Circular No. 2013-001 (Approval of the Philippine National Public Key Infrastructure [PNPKI] Certificate Policy Version 1.0) and the Memorandum Circular No. 2013-002 (Approval of the PNPKI Certification Authority [CA] Certification Practice Statement [CPS] Version 1.0).

3.2 Abbreviations

Term	Description
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit
TST	Time-Stamp Token
UTC	Coordinated Universal Time
TSS	Time-Stamping Service
CA	Certification Authority
CP / CPS	Certificate Policy / Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Service Provider
OCSP	Online Certificate Status Protocol
PNPKI	Philippine National Public Key Infrastructure

4. General Concepts

4.1 Time-Stamping Services

Component services that make up the Time-Stamping Services (TSSs) are as follows:

a) **Time-Stamping Provision** – This is the component that generates TSTs with authoritative time and date values.
b) **Time-Stamping Management** – This component monitors and controls the operation of the TSSs to ensure that the service is properly provided. This service component is responsible for the installation and de-installation of the time-stamping provision service. Time-stamping management ensures that the clock used for time-stamping is correctly synchronized with UTC.

The PNPKI TSA guarantees the integrity and reliability of the TSSs and its components.

4.2 Time-Stamping Authority

The PNPKI TSA is trusted by subscribers and relying parties in issuing secure and accurate TSTs. The PNPKI TSA has overall responsibility for TSSs identified in Section 4.1 (Time-Stamping Services) of this document. The PNPKI TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the PNPKI TSA. The PNPKI TSA is identifiable in the issued TSTs (refer to Section 7.3, Time-Stamp Token, of this document).

4.3 Subscriber

The subscriber refers to either an individual or an organization that have agreed to the PNPKI Subscriber Agreement.

- When the subscriber is an individual, he / she will be held directly responsible if his / her obligations are not correctly fulfilled.

- When the subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore the organization is expected to suitably inform its end-users.

4.4 Time-Stamp Policy and TSA Practice Statement

4.4.1 Purpose

The purpose of this document is to specify the time-stamp policy to meet general requirements for trusted time-stamping services. The PNPKI TSA specifies in its practice statement how these requirements are met.

4.4.2 Level of Specificity

When compared to the PNPKI TSA time-stamp policy, the PNPKI TSA practice statement is more specific. It is a more detailed description of the terms and conditions as well as business and operational practices of the PNPKI TSA in issuing and managing TSSs. The PNPKI TSA practice statement enforces the rules described by the PNPKI TSA time-stamp policy. The PNPKI practice statement defines how the PNPKI TSA meets the organizational, procedural, as well as technical requirements identified in the PNPKI TSA time-stamp policy.

4.4.3 Approach

The PNPKI TSA time-stamp policy is defined independently of the specific details of the operating environment of the PNPKI TSA. The PNPKI TSA practice statement is tailored to the PNPKI TSA's organizational structure, facilities, operating procedures, as well as computing environment.

5. Time-Stamp Policies

5.1 Overview

This PNPKI TSA-TSP is a named set of rules that indicates the applicability of a TST to a particular community and / or class of application with common security requirements, which include among others:

- The TSU, private keys, and profiles of public key certificates are in compliance with technical specifications of the RFC 3161 and RFC 3628.
- The PNPKI TSA holds private keys used in signing time-stamps.
- TSTs are issued with the accuracy of ± 1 second, as indicated in Section 6.1.2 (TSA Obligations Towards Subscribers) and Section 7.1.2 (TSA Disclosure Statement).
- Means used in requesting for time-stamps include the Transfer Control Protocol (TCP) and Hypertext Transfer Protocol (HTTP).

This document, the PNPKI TSA-TSP/PS, can be accessed via http://i.gov.ph/pki/policies/.

5.2 Identification

The object identifier (OID) for the PNPKI TSA-TSP/PS is: 2.16.608.1.20.1.1.

The OID is referenced in every time-stamp issued by the PNPKI TSA.

5.3 User Community and Applicability

The PNPKI TSA's User Community is composed of subscribers and relying parties. Accordingly, subscribers are also regarded as relying parties.

This PNPKI TSA-TSP is aimed at meeting the requirements of time-stamping qualified digital signatures for long term validity, but is generally applicable to any requirement for an equivalent quality.

This policy does not define restrictions on the applicability of the time-stamps issued. The only exceptions are those stated under Section 1.4.2 (Prohibited Certificate Usage) of the PNPKI CPS.

5.4 Conformance

To show conformance with this document, the PNPKI TSA uses the identifier for the time-stamp policy established in Section 5.2 (Identification) of this document in its issued TSTs.

The PNPKI TSA is subject to periodic independent internal and external audits. The PNPKI TSA guarantees conformance of its implemented controls with Section 7 (Requirements on TSA Practices) and ensures that it meets its obligations specified in Section 6.1 (TSA Obligations) of this document.

6. Obligations and Liability

6.1 TSA Obligations

6.1.1 General

This section describes the obligations, liabilities, guarantees, and responsibilities of the PNPKI TSA, subscribers, and relying parties. Obligations and responsibilities are defined and regulated in mutual agreements and obligations between the PNPKI TSA and subscribers.

The PNPKI TSA ensures that the procedures described in Section 7 (Requirements on TSA Practices) of this document are undertaken.

6.1.2 TSA Obligations Towards Subscribers

The PNPKI TSA undertakes the following obligations towards subscribers:

a) To operate in accordance with this PNPKI TSA-TSP/PS, the PNPKI CP/CPS, and other relevant operational policies and procedures;
b) To ensure that TSUs maintain a minimum UTC time accuracy of ± 1 second;
c) Undergo internal and external reviews to assure compliance with relevant legislation and internal PNPKI policies and procedures; and

d) To provide high availability access to PNPKI TSA systems except in the case of planned technical interruptions or loss of time synchronization.

6.2 Subscriber Obligations

Subscribers have the following obligations:

a) To verify if the TST has been correctly signed; and
b) To verify if the private key used to sign the TST has not been compromised.

6.3 Relying Party Obligations

Before trusting on TSTs, Relying Parties shall do the following:

a) Verify that the TST has been correctly signed and that the private key used to sign the TST has not been compromised until the time of verification; and
b) Take into consideration any limitations on the usage of the TST indicated by the time-stamp policy.

6.4 Liability

The PNPKI TSA undertakes to operate in accordance with this PNPKI TSA-TSP/PS, the PNPKI CP/CPS, and the terms of agreements with the subscriber. The PNPKI TSA makes no express or implied representations or warranties relating to the availability or accuracy of the time-stamping services. The PNPKI TSA shall not in any event be liable for the following:

a) Loss of profits;
b) Loss of sales or turnover;
c) Loss or damage to reputation;
d) Loss of contracts;
e) Loss of customers;
f) Loss of the use of any software or data; or
g) Losses or liabilities under or in relation to contracts.

The term "loss" means a potential loss or reduction in value as well as a complete or total loss.

The PNPKI TSA bears specific liabilities for damage to subscribers and relying parties in relationship to valid qualified Digital Certificates relied upon in accordance with specific national laws and regulations. These liabilities are described in Section 9.8 (Limitations of Liability) of the PNPKI CP/CPS.

7. Requirements on TSA Practices

To assure the integrity and reliability of the TSSs, the PNPKI TSA shall need to implement controls.

7.1 Practice and Disclosure Statements

7.1.1 TSA Practice Statement

Once a year, the PNPKI TSA shall assess the vulnerability of its system or its components. A routine risk assessment of the system shall be performed regularly for evidence of any malicious activity. This is also to determine the necessary security controls and operational procedures.

The terms and conditions on the use of the TSSs of the PNPKI TSA are made available to all subscribers and relying parties, as described in Section 7.1.2 (TSA Disclosure Statement) of this PNPKI TSA-TSP/PS.

This PNPKI TSA-TSP/PS, along with the PNPKI CP/CPS and other public documents are found at http://i.gov.ph/pki/policies/. Internal documents shall only be made available to authorized personnel and to auditors of the PNPKI TSA, under strictly controlled conditions. Should there be any changes in this document, subscribers and relying parties will be given due notice.

This document and the PNPKI CP/CPS identify the obligations, liabilities, guarantees, and responsibilities of the PNPKI TSA, subscribers, and relying parties.

The ICT Office is responsible for all aspects of this PNPKI TSA-TSP/PS, and the PNPKI CP/CPS, according to the provisions of Section 1.5 (Policy Administration) of the PNPKI CPS.

7.1.2 TSA Disclosure Statement

The PNPKI TSA shall disclose to all its subscribers and relying parties the terms and conditions in connection with the use of the TSSs. This TSA Disclosure Statement shall also be described in the PNPKI Subscriber Agreement.

The PNPKI TSA ensures that all the issued TSTs include the identifier specified in Section 5.2 (Identification) of this document.

In this document, the time accuracy of the TSTs is indicated in Section 6.1.2 (TSA Obligations Towards Subscribers) and the liabilities in Section 6.4 (Liability).

The expected validity period of every TST is two years. The TSTs will be archived for the duration of two years, starting from the time mentioned in the TSTs. The PNPKI TSA maintains secure records concerning the operation

of the PNPKI TSA according to Section 5.5 (Records Archival) of the PNPKI CPS.

Limitations related with the TSA system are described in Section 5.3 (User Community and Applicability) of this document. The subscriber's obligations are defined in Section 6.2 (Subscriber Obligations) and the relying party's obligations are indicated in Section 1.3 (Relying Party Obligations).

The cryptographic algorithms and key lengths used by the PNPKI TSA are as follows:

- Acceptable Time Stamp request Hash: sha256WithRSAEncryption
- Signature: sha256WithRSAEncryption

Complaints and dispute settlements shall be addressed to the following contact information:

Philippine National PKI
ICT Office-NCC Building
Carlos P. Garcia Avenue
U.P. Campus, Diliman
1101 Quezon City, PHILIPPINES
Tel. No.: (+632) 920-0101
Fax No.: (+632) 920-7414

7.2 Key Management Life Cycle

7.2.1 TSA Key Generation

The PNPKI TSA ensures that any cryptographic keys are generated within a Hardware Security Module (HSM) that meets Level 3 of the Federal Information Processing Standard 140-2 (FIPS 140-2) by authorized personnel identified in Section 5.2.1 (Trusted Roles) of the PNPKI CPS.

Generation of keys is in compliance with Section 6.1 (Key Pair Generation and Installation) of the PNPKI CPS.

7.2.2 TSU Private Key Protection

The PNPKI TSA ensures that the TSU private keys remain confidential and maintain their integrity by taking particular steps. These steps include generating, holding, and using the TSA keys within the HSM that complies with FIPS 140-2, Level 3, by personnel listed in Trusted Roles of the PNPKI CPS within a physically secured and controlled environment.

When performing a TSA key back up and key recovery during a failure of the system or a disaster, the procedures shall be in conformance with those that are described in the PNPKI CPS.

7.2.3 TSU Public Key Distribution

The TSU signature verification public keys must be delivered securely towards relying parties. Additional information is detailed in Section 6.1 (Key Pair Generation and Installation) of the PNPKI CPS.

7.2.4 Rekeying TSU's Key

Before the validity period is reached, specifically when the algorithm or key size is considered to be unsafe, the TSU private signing keys need to be replaced. Procedures identified in Section 4.6 (Certificate Renewal) and Section 4.7 (Certificate Re-Key) of the PNPKI CPS shall be followed.

7.2.5 End of TSU Key Life Cycle

To ensure that TSU private signing keys are not used upon their expiration, e.g., in issuing TSTs once the private keys have expired, these keys are replaced. Likewise, TSU private keys, or any key part, that have expired are destroyed, following the steps identified in Section 6.2.10 (Method of Destroying Private Key) of the PNPKI CPS. The TST generation system shall reject any attempt to issue TSTs if the signing private key has expired.

7.2.6 Life Cycle Management of the Cryptographic Module used to Sign Time-Stamps

The PNPKI TSA shall follow procedures and controls, in accordance with the PNPKI CPS, to ensure that the TST signing cryptographic hardware for the non-repudiation services are not tampered with during shipment or storage.

Acceptance testing shall be performed to check if the cryptographic hardware is functioning correctly.

The installation, activation, and duplication of TSU's signing keys in the HSM shall be executed by personnel in the Trusted Roles within a physically secured environment. Upon the retirement of the TSU HSM, the private keys stored on it shall be erased.

7.3 Time-Stamping

7.3.1 Time-Stamp Token

The PNPKI TSA ensures that the TSTs are issued securely, following the provisions of Section 7.2.3 (TSU Public Key Distribution) of this document and Section 6.1 (Key Pair Generation and Installation) of the PNPKI CPS, and include the correct time.

Each of the TSTs issued by the PNPKI TSA shall include the following:

a) A unique object identifier of the policy as described in Section 5.2 (Identification) of this document;
b) The time values identifiable to the real UTC time value;
c) An identifier for the TSA and the TSU;
d) An electronic signature generated using a key used exclusively for this time-stamping purpose;
e) A unique serial number that can be used to both order TSTs and to identify particular TSTs; and
f) A representation of the datum being time-stamped as provided by the requestor.

7.3.2 Clock Synchronization

The PNPKI TSA ensures that clock synchronization with UTC and / or the Philippine Standard Time (Republic Act No. 10535, s. 2012) is maintained within the declared accuracy. The time accuracy is defined in Section 6.1.2 (TSA Obligations Towards Subscribers).

Security and technical measures are in place to prevent any manipulation to the TSU clocks. The clocks are protected within the HSMs. These clocks can also detect time drift outside preset boundaries and request additional recalibrations as needed. Recalibrations are conducted at least twice a day against the reference time source. Should the TSU clock drifts outside the declared accuracy, and recalibration fails, the PNPKI TSA shall not issue time-stamps until the correct time is restored.

Manual administration of these clocks is performed by authorized personnel listed in Section 5.2.1 (Trusted Roles) of the PNPKI CPS.

7.4 TSA Management and Operation

7.4.1 Security Management

The PNPKI TSA assures that administrative and management procedures implemented are according to the recognized best practices and the requirements of applicable standards.

All requirements and subjects related to security management are applied in accordance with Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the PNPKI CPS.

7.4.2 Asset Classification and Management

The PNPKI TSA assures that its information and other assets receive an appropriate level of protection. Procedures and measures on ensuring the stability of the TSA system operation are applied. The PNPKI TSA maintains an inventory of all its assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

More information is described in Section 6.6 (Life Cycle Technical Controls) of the PNPKI CPS.

7.4.3 Personnel Security

In order to maintain the trustworthiness of the PNPKI TSA's operations, appropriate personnel and hiring practices that comply with security best practices as well as the requirements of applicable standards shall be maintained.

Detailed information relevant to personnel security can be found in Section 5 (Management, Operational and Physical Controls) and Section 6 (Technical Security Controls) of the PNPKI CPS.

7.4.4 Physical and Environmental Security

The PNPKI TSA ensures that the location and construction of the facility housing the TSA equipment are consistent with facilities to house high value, sensitive information. The application of physical and environmental security shall be in conformance with Section 5.1 (Physical Security Controls) of the PNPKI CPS.

7.4.5 Operations Management

In order to minimize the risk of failure, the PNPKI TSA maintains an internal documentation specifying the extensive operational controls, processes, procedures, and infrastructure. This documentation shall only be made available to the PNPKI TSA auditors on a periodic basis.

The operations management for the PNPKI TSA is covered by the overall PNPKI operations management controls. More specific information in regard to Operation Management is defined in Section 5 (Management, Operational and Physical Controls).

7.4.6 System Access Management

Appropriate physical and logical PNPKI TSA system access controls shall only be limited to authorized individuals identified in the PNPKI CPS.

7.4.7 Trustworthy Systems Deployment and Maintenance

The PNPKI TSA ensures that it uses trustworthy systems and products that are protected against modifications, thereby performs activities such as:

a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the PNPKI TSA or on behalf of the PNPKI TSA to ensure that security is built into IT systems.
b) Change control procedures shall be applied for releases, modifications, and emergency software fixes of any operational software.

Systems development and maintenance controls for the PNPKI TSA are in accordance with the provisions of the PNPKI CPS. Specific information is provided in Section 6 (Technical Security Controls) of the PNPKI CPS.

7.4.8 Compromise of TSA Services

In the event of compromise of a TSU private key, the PNPKI TSA will follow the procedures outlined in Section 5.7 (Compromise and Disaster Recovery) of the PNPKI CPS. This includes revoking the relevant Certificate and adding it to the PNPKI TSA CRL. The TSU will not issue time-stamps if its private key is not valid. The TSU will not issue time-stamps if its clock is outside the declared accuracy from reference time source, until steps are taken to restore calibration of time.

7.4.9 TSA Termination

In the event that the PNPKI TSA terminates its operation, it shall adhere to the procedures outlined in Section 5.8 (CA or RA Termination) of the PNPKI CPS.

7.4.10 Compliance with Legal Requirements

The PNPKI TSA ensures compliance with any applicable laws or legal requirements.

7.4.11 Recording of Information Concerning Operation of Time-Stamping Services

The PNPKI TSA shall comply with its records retention policy in accordance with applicable laws and Section 12.2 of DTI DA 10-09, series 2010, as stated in Section 5.5 (Records Archival) of the PNPKI CPS.

Specifically, the PNPKI TSA maintains records, with precise time, of the following:

a) Time stamped requests and created time-stamps;
b) Events related to TSA administration, which includes the following: clock synchronization, certificate management, and key management; and
c) Events related to the life-cycle of a TSU key and Certificate.

7.5 Organizational

The PNPKI TSA ensures that its organization is reliable.

Policies and practice statements, including this document, for the PNPKI is found at http://i.gov.ph/pki/policies/. Other internal documents describing specific details about the PNPKI TSA shall be made available only under strictly controlled conditions.

8. Certificate Profile

The Certificate Profile for the PNPKI TSA is described as follows:

TSA Certificate (Time-stamp Signing Certificate Profile)				
Base Certificate				
Certificate	OID	Include	Critical	Value
Signature Algorithm				
Algorithm		x		sha256WithRSAEncryption
Signature Value		x		Issuing CA Signature
TSA Certificate				
Version		x		3
Serial Number		x		Provided by the CA (validated on duplicates)
Signature		x		sha256WithRSAEncryption
Validity				
Not Before		x		Key Generation Process Date
Not After		x		Key Generation Process Date + 730 days
Subject Public Key Info		x		Provided by PKCS10 request – key length 2048
Issuer				
Country		x		PH
Common Name		x		Gov Signing CA
Organization Name		x		DOST

Subject			Required	
Common Name		x	YES	Time Stamp Signer 1
Country Name		x	YES	PH
eMail				
Subject Serial Number		x		Provided by the CA
Locality				
State or Province				
Organization Unit				
Organization		x	YES	DOST
Standard Extensions	**OID**	**Include**	**Critical**	**Value**
Certificate Policies			0	
Policy Identifier		x		2.16.608.1.20.1.1
Policy Qualifiers		x		None
Policy Qualifier Id		x		CPS
Qualifier				
Display Text				
Key Usage			1	
Non Repudiation		x		Set
Digital Signature				
Extended Key Usage			1	
Time stamping		x		Set
Subject Alternative Name			0	
822 Email Address				
Basic Constraints			0	
CA		x		FALSE

Modification History

Version	Effective Date	Changes
1.0	August 8, 2014	