Subscriber Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT support.pnpki@dict.gov.ph.

1.0 Definitions

Applicant: The individual that applies for (or seeks renewal of) a Digital Certificate naming it as the "Subject".

Certification Practice Statement (CPS) – A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

Certificate Policy (CP) – A named set of rules that indicate s 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.

Certificate Revocation List ("CRL"): A collection of electronic data containing the list of serial numbers revoked or suspended by the Certificate Authority

Online Certificate Status Protocol ("OCSP"): An Internet Protocol (IP) used to obtain the real time revocation status of a digital certificate. It is used as an online faster alternative to CRL list.

Public Key – A mathematical key which is available publicly and which is used to verify Digital Signatures created with the matched Private Key and to encrypt electronic data which can only be decrypted using the matched Private Key

Private Key: A mathematical key which is kept private to the owner and which is used to create Digital Signatures or to decrypt electronic data

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).

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

2.0 Authority to Use Digital Certificates

2.1 Grant of Authority

As from the Effective Date up to the validity period of any issued Digital Certificate ("Valid from" date to "Valid to" date), PNPKI grants to the Subscriber the authority to use the requested

Digital Certificate in conjunction with Private Key and/or Public Key operations. The obligations of the subscriber (see section 4.0) with respect to Private Key protection are applicable from the effective date.

2.2 Limitations on Authority

The digital certificate cannot be used for purposes other than what is allowed in this subscriber agreement and the CPS.

3.0 Use of PNPKI Digital Certificate

The subscriber shall use the certificate for its lawful and intended use only. The certificate shall be used in accordance with its Key-Usage field extensions. All issued certificate by PNPKI cannot be used for purposes other than what is allowed in this subscriber agreement and by the CPS. PNPKI shall not be liable for any claims arising from prohibited use.

3.1 Acceptance of a Digital Certificate

The following conduct constitutes certificate acceptance:

a) A certificate shall be deemed accepted when it is in the subscriber or representative's control;

b) Failure of the subscriber to object to the certificate or its content within five (5) calendar days; or

c) The subscriber uses the certificate.

3.2 Revocation of Digital Certificates

A certificate shall be revoked when the bind between the subject and the subject's public key is no longer valid.
An end-user subscriber certificate can be requested for revocation under any of the following conditions:

a) When a verified request for revocation is received by PNPKI CA or RA;

b) When any of the information found in the certificate is changed or no

longer applicable;

c) When the Private Key, or the media holding the Private Key, associated with the certificate is compromised;

d) When the PNPKI CA determines that the end-user entity is no longer complying with the requirements of by the CPS and this subscriber agreement; or

e) When the PNPKI CA has the reason to believe that the certificate was issued in a manner that is not in accordance with the procedures required by the CPS and this subscriber agreement.

g) When subscriber requested revocation of the Certificate;

4.0 Subscriber Obligations

This Agreement governs the subscriber's application for, acceptance, and use of, a digital certificate issued by the RA.

a. The provisions of the Root CA CP/CPS, GovCA CP/CPS, and other pertinent documents are binding upon the subscriber.

b. All the information provided in the digital certificate application form is true and correct.

c. The use of the digital certificate shall be for the sole use of the subscriber.

d. The subscriber will not, under any circumstances, allow any other person to use the digital certificate. Any such use by another person constitutes a compromise of the associated private key, requiring the revocation of the digital certificate.

e. The subscriber shall protect the confidentiality of the private key associated with his or her digital certificate as well as any PIN number or other means used to activate the private key.

f. The subscriber shall remain solely responsible for the maintenance of the confidentiality of the certificate.

g. The subscriber shall not use the digital certificate for any unlawful purpose, or for any purpose that does not have anything to do with accessing the PKI information systems or transactions using the digital certificates.

h. The subscriber shall promptly request the RA to revoke the digital certificate upon knowing or suspecting inaccurate information, loss, exposure or compromise of the associated private key.

i. The subscriber shall not tamper, interfere with, or reverse-engineer any technical implementation of the digital certificate or its use, or in any manner seek to compromise the security provided by the RA and the National PKI system.

j. The subscriber accepts the risk of an undetected compromised digital certificate or associated private key, which may be used to impersonate the said subscriber.

5.0 Permission to Publish Information

The Subscriber agrees that PNPKI may publish the serial number of the Subscriber's Digital Certificate in connection with PNPKI's dissemination of CRL's and OCSP.

6.0 Disclaimer

PNPKI shall not be liable for any claims arising from prohibited use of Digital Certificates issued by GovCA. PNPKI will not be liable if the user has not respected his obligations mentioned in the CPS and in this agreement.

7.0 Term and Termination

This agreement shall terminate upon

(a) The expiry date of any Digital Certificate issued to the Subscriber

(b) Any failure to comply with any of the subscriber obligations mentioned in this Subscriber Agreement

8.0 Effect of termination

Upon termination of this Subscriber Agreement for any reason, PNPKI may revoke the Subscriber's Digital Certificate in accordance with PNPKI revocation procedures.

9.0 CP and CPS Information

The digital certificate contains information provided by the subscriber, which is authenticated by the RA in accordance with the requirements set out in the CA CP and CPS, available for viewing and download at dict.gov.ph/pnpki/.

Modification History

Version	Effective Date	Changes
1.0	June 3, 2015	Created Digital Certificate Subscriber Agreement version 1.0
2.0	March 18, 2019	Amendment of Digital Certificate Subscriber Agreement version 1.0 to reflect the change of administering authority from iGovPhil to the Department of Information and Communications Technology. Changed support email from pkisupport@i.gov.ph to support.pnpki@dict.gov.ph Revised Section 9.0 CP and CPS Information, changed www.i.gov.ph/services/publickeyinfrastructure/ to dict.gov.ph/pnpki/