



Republic of the Philippines
Department of Education
REGION VI – WESTERN VISAYAS
SCHOOLS DIVISION OF AKLAN

August 9, 2021

DIVISION MEMORANDUM
No. 278, s. 2021

**APPLICATION OF FIELD OFFICES AND SCHOOL PERSONNEL FOR PNPKI
DIGITAL SIGNATURE**

To: OIC, Office of the Assistant School Division Superintendent
Chief Education Supervisors
Education Program Supervisors
Public Schools District Supervisors
Senior/Education Program Specialists
Heads of Public and Private Elementary, Secondary
and Integrated Schools
All Others Concerned

1. Attached are Regional Memorandum No. 435, s. 2021 and OUA MEMO No. 00-0721-0129 and 00-0721-0169 from the Office of the Undersecretary for Administration (OUA) titled **Application of Field Offices and School Personnel for PNPKI Digital Signature**.
2. Immediate dissemination of this Memorandum is desired.


MIGUEL MAC D. APOSIN, EdD, CESO V
Schools Division Superintendent

Enclosure : RM No. 435, s. 2021, OUA Memos 00-0721-0129 and 00-0721-0169

Reference : As stated

To be indicated in the Perpetual Index
under the following subjects:

PNPKI
LMS
ICT

MMDA/srb



Poblacion, Numancia, Aklan
Tel/Fax No. (036) 265 3744 | (036) 265 3737 | (036) 265 3738
Website: <http://www.depedaklan.org>
Email Address: aklan.1958@deped.gov.ph



Republic of the Philippines
Department of Education
REGION VI – WESTERN VISAYAS

REGIONAL MEMORANDUM

No. 435 s.2021

**APPLICATION OF FIELD OFFICES AND SCHOOL PERSONNEL FOR PNPKI
DIGITAL SIGNATURE**

**To: Schools Division Superintendents
All Others Concerned**

1. Attached are the OUA Memos 00-0721-0129 and 00-0721-0169 from the Office of the Undersecretary for Administration, regarding the **Application of Field Offices and School Personnel for PNPKI Digital Certificates**.
2. Immediate dissemination of this Memorandum is desired.


RAMIR B. UYTICO EdD, CESO IV
Regional Director

Enclosure : OUA Memos 00-0721-0129 and 00-0721-0169

Reference : As stated

To be indicated in the Perpetual Index
under the following subjects:

PNPKI
LMS
ICT



Address: Duran Street, Iloilo City, 5000
Telephone Nos: (033)509-7653; (033)336-2816
Email Address: region6@deped.gov.ph
Website: region6.deped.gov.ph

Document Name	Document No.	Date Created	Revision Number
Regional Memorandum	DepEd RO6-ORD-ICT-RM 009	08/03/2021	00





OUAD00-0721-0129
To authenticate this document,
please scan the QR Code



Republika ng Pilipinas
Kagawaran ng Edukasyon
Tanggapan ng Pangalawang Kalihim

OUA MEMO 00-0721-0129
MEMORANDUM
16 July 2021

For: **Regional Directors and BARMM Education Minister**
Schools Division Superintendents
Region and Division Information Technology Officers
Region and Division Personnel Officers
Public School Heads
All Others Concerned

Subject: **APPLICATION OF FIELD OFFICES AND SCHOOL**
PERSONNEL FOR PNPKE DIGITAL SIGNATURE

The Department of Education (DepEd) through the Bureau of Human Resources and Organizational Development (BHROD) and the Information and Communications Technology Service (ICTS), in partnership with the Department of Information and Communications Technology (DICT), has started processing applications for the Philippine National Public Key Infrastructure (PNPKI) Digital Signature.

"Public Key Infrastructure (PKI) allows users of public networks like the Internet to exchange private data securely. PKI is essentially a set of hardware, software, policies, personnel, and procedures needed to create, manage, distribute, use, store and revoke digital certificates. The PKI is one of the core services being offered by the Department of Information and Communications Technology (DICT) that will foster trust in the government by ensuring secure and reliable online transactions." (Source: <https://dict.gov.ph/pnpki/>)

At the outset, this initiative is expected to

1. support business as usual without sacrificing the safety of signatories and employees routing physical documents;
2. foster trust between offices by ensuring secure and reliable online transactions;
3. successfully integrate the use of digital signatures in the process flow and vastly increase acceptance on the integrity of official documents within and outside the Department; and
4. prevent the transmission of COVID-19 on widely used official documents.



Office of the Undersecretary for Administration (OUA)

[Administrative Service (AS), Information and Communications Technology Service (ICTS), Disaster Risk Reduction and Management Service (DRMMS), Bureau of Learner Support Services (BLSS), Baguio Teachers Camp (BTC), Central Security & Safety Office (CSSO)]

Department of Education, Central Office, Meralco Avenue, Pasig City
Rm 519, Mabini Bldg; Mobile: +639260320762; Tel: (+632) 86337203, (+632) 86376207
Email: usec.admin@deped.gov.ph; Facebook/Twitter @depedtayo



Scan this QR Code to view
Videos and Magazines
of Major Programs



Normally, government employees are instructed to apply individually and produce the needed requirements. However, due to the huge number of DepEd personnel, DICT has granted processing of applications through bulk registration. While waiting for updates on the request to waive all the needed requirements, **all DepEd personnel are advised to fill-out the application form.**

Currently, DepEd is processing the application of the Management Committee (MANCOM) members, Central Office personnel with procurement-related roles and DepEd PNPKE Secretariat.

To expedite the process in the field, **especially for those who will serve in the 2022 National and Local Elections**, the following activities will be conducted:

1. Virtual orientation and demonstration on the use of the **Learning Management System (LMS)**
2. Asynchronous (or self-paced) virtual orientation and **submission of PNPKE requirements through the LMS**

Note: Both activities will run from **29 July to 25 August 2021**. More details will be provided in a separate Memorandum.

The **Regional Information Technology (IT) Officers** are hereby designated as the **Regional PNPKE Focal Persons**, while **Division IT Officers** shall be the **Division PNPKE Team Leads**, effective immediately. **Regional and Division Personnel Officers** will also form part of the **PNPKE Team**. The responsibilities and duties of the PNPKE Team will be issued in a separate Memorandum.

The DepEd PNPKE Resources such as forms, guides and samples are already available at <http://bit.ly/Deped-PNPKE> . The content on this link including the process flow and other materials will be regularly updated before the start of activities.

For more information, questions and concerns on this subject, kindly contact Ms. Niña Rica Bernas, Technical Assistant II of the ICTS – User Support Division (USD), through Microsoft Teams or email at support.pnpki@deped.gov.ph

For immediate and appropriate action.

ALAIN DEL B. PASCUA
Undersecretary



OUAD00-0721-0129
To authenticate this document,
please scan the QR Code



2



OUAD00-0721-0169
To authenticate this document,
please scan the QR Code



Republika ng Pilipinas
Kagawaran ng Edukasyon
Tanggapan ng Pangalawang Kalihim

OUA MEMO 00-0721-0169
MEMORANDUM
26 July 2021

For: **Regional Directors and BARMM Education Minister**
Schools Division Superintendents
Region and Division IT Officers
Region and Division Personnel Officers
School Heads
All Others Concerned

Subject: **ADDENDUM TO THE MEMORANDUM ON THE APPLICATION OF FIELD OFFICES AND SCHOOL PERSONNEL FOR PNPKEI DIGITAL CERTIFICATES**

The Commission on Election's (COMELEC) *Policy Guidelines on the Implementation of Digital Certificate for the 2022 National and Local Elections and Bangsamoro Autonomous Region of Muslim Mindanao Elections* requires the use of digital signatures for personnel who will serve in the May 2022 National and Local Elections to ensure transparency and credibility.

In relation to this, the Office of the Undersecretary for Administration (OUA) releases this addendum to OUA Memo 00-0721-0129 *Application of field offices and school personnel for PNPKEI digital signature* released on 16 July 2021.

The Department of Information and Communications Technology (DICT) has extended their full support by allowing DepEd to process the application for digital certificates through bulk registration and has waived the submission of requirements that are otherwise too taxing to provide, considering that DepEd personnel who will serve in the election **must have digital certificates on or before the 30th of September 2021**.

For the prioritization list in the processing of applications and composition of the PNPKEI Team, please refer to **Annex A**.

For the steps and details on the application process, refer to **Annex B**.



Scan this QR Code to view
Videos and Magazines
of Major Programs



Office of the Undersecretary for Administration (OUA)

[Administrative Service (AS), Information and Communications Technology Service (ICTS), Disaster Risk Reduction and Management Service (DRRMS), Bureau of Learner Support Services (BLSS), Baguio Teachers Camp (BTC), Central Security & Safety Office (CSSO)]

Department of Education, Central Office, Meralco Avenue, Pasig City
Rm 519, Mabini Bldg; Mobile: +639260320762; Tel: (+632) 86337203, (+632) 86376207
Email: usec.admin@deped.gov.ph; Facebook/Twitter @depeditayoy

In relation to the application process, the following asynchronous (or self-paced) virtual orientations and demonstration activities will be conducted:

1. The use of the **Learning Management System (LMS)**.
2. **Submission** of PNPKI requirements **through the LMS**.


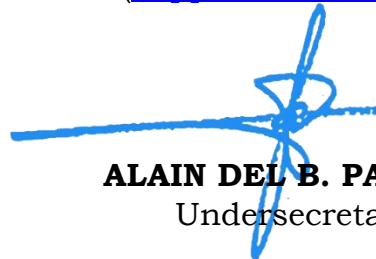
Note: Both activities will run from **29 July to 25 August 2021**.

DepEd PNPKI Resources such as forms, guides, and samples are already available through this link: <http://bit.ly/Deped-PNPKI>. Contents of this resource, including process flows and other materials, will be regularly updated.

For any questions and concerns, please contact the following personnel through email or chat via MS Teams:

- PNPKI concerns – Ms. Niña Rica Bernas (support.pnpki@deped.gov.ph)
- LMS concerns – Mr. Winifredo Valdez (support.usdlms@deped.gov.ph)

For immediate compliance.


ALAIN DEL B. PASCUA
Undersecretary



OUAD00-0721-0169
To authenticate this document,
please scan the QR Code



Annex A

PRIORITIZATION OF DEPED PERSONNEL FOR PNPKI DIGITAL CERTIFICATE APPLICATION

1. Prioritization

DepEd personnel who are currently or will be involved in the following shall be prioritized:

- The 2022 National and Local Elections
 - COMELEC stated that DepEd personnel who will serve in the 2022 elections should have the PNPKI-digital certificate by September 2021.
- Signatories of procurement-related activities
 - Head of the Procuring Entity;
 - Bids and Awards Committee Member;
 - Technical Working Groups;
 - BAC Secretariat; and
 - End-users/Implementing Units.
- Members of the DepEd PNPKI Team in all governance levels.
- Other activities that require immediate use of PNPKI-certified digital certificate.

2. Regional PNPKI Team (i.e., PNPKI Focal Person, etc.)

Regional offices will have the flexibility to arrange the schedules when their respective SDOs may access the portal.

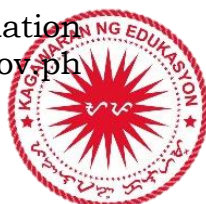
The composition of the Regional and Division PNPKI Teams are as follows:

a. Regional Directors

- Responsibilities
 - Oversee the activities, status of submissions, and other related activities.
 - Provide the support needed by the PNPKI Teams to reach at least 90% of the personnel in the priority list and at least 75% of personnel in the region with PNPKI digital certificate by September 2021.

b. Regional Information Technology Officers (RITOs)

- Officially designated as **PNPKI Focal Person and Team Leader of Regional PNPKI Team** effective immediately.
- RITOs are instructed to update and submit the following information through email to Mr. Hubert Cordial at hubert.cordial@deped.gov.ph **on or before 23 July 2021:**



- Complete Name, Position, DepEd email address, and contact number/s.
- Responsibilities
 - In-charge of ensuring that all identified entities in this memorandum will be oriented to apply for their PNPKI-certified digital certificate.
 - Setup and manage Regional LMS servers.
 - Coordinate with the PNPKI Cluster Team Office assigned in their respective regions.
 - May opt to add member/s to the Regional PNPKI Team as needed.
 - Report to DepEd Central Office via **support.pnpki@deped.gov.ph** the status of the number of applications submitted thru the LMS.
 - Assist in resolving issues and concerns in relation to the activity.

c. **Regional Administrative Officer Personnel**

- Officially designated as **Regional PNPKI Team members** effective immediately.
- Responsibilities:
 - Support and assist the **Regional Focal Person** in the execution of responsibilities.
 - Support and assist the **Regional PNPKI Team** in the scheduling of the personnel within the Regional Office.
 - Assist in resolving issues and concerns in relation to the activity.

d. **Division Information Technology Officers (DITOs)**

- Officially designated as **Regional PNPKI Team member** and **Division PNPKI Team Lead** effective immediately.
- Responsibilities
 - Assist the **Regional PNPKI Team** in coordinating and ensuring the cooperation of the whole division in achieving the objectives of the activity.
 - Coordinate and assist the **Regional PNPKI Team** in finalizing LMS training schedules for their respective division.
 - May opt to add member/s to the **Division PNPKI Team** as needed.
 - Coordinate and assist the applicants on how to fill-out the application form and other requirements.
 - Assist in resolving issues and concerns in relation to the activity.



e. **Division Administrative Officer Personnel**

- Officially designated as Division PNPKI Team members effective immediately.
- Responsibilities:
 - Support and assist the **Division PNPKI Team Lead** in the execution of responsibilities.
 - Support and assist the **Division PNPKI Team** in the scheduling of the personnel within the Regional Office.
 - Assist in resolving issues and concerns in relation to the activity.

3. Data Privacy

- To protect the handling of personal information that will be used in this endeavor, only those recognized DepEd personnel will be able to transact with PNPKI offices and personnel.
- It is the responsibility of the members of the Regional and Division PNPKI Teams to **secure** the submitted requirements of all applicants in compliance with the Data Privacy Act.



Annex B

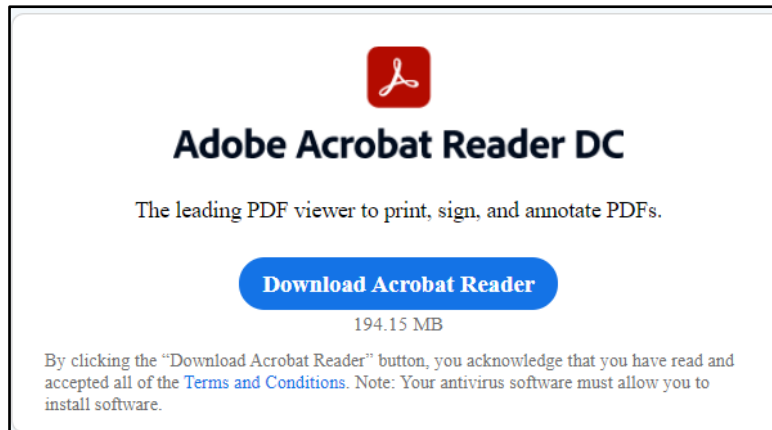
STEPS IN BULK APPLICATION FOR PNPKI DIGITAL CERTIFICATE

This is for DepEd Field Office personnel who will apply through bulk application done thru the DepEd Learning Management System (LMS.)

Steps in applying for the PNPKI digital certificate:

1. Preparatory activities prior to applying for the PNPKI digital certificate are as follows:
 - a. Secure a soft copy of clear and decent passport-sized ID picture
 - 4.5 cm x 3.5 cm or 1.8 inches x 1.4 inches.
 - Picture should show the whole head up to the shoulders.
 - Clear (not blurred) and high-resolution picture (min. of 600 dpi)
 - When taking the picture using a smartphone, ensure that the resolution is set at the highest setting and with ample lighting.
 - Image should be in either JPG or PNG format.
 - Taken within the last six (6) months
 - Stretched images will not be considered
 - b. Secure soft copy of electronic signature
 - Using a black permanent marker or any writing instrument with a broad and continuous even ink flow, write a big sample of your signature on a piece of white paper.
 - Ensure that the sample signature is very clear and matches your official signature.
 - After making the sample signature, have it scanned in high resolution (minimum of 600 dpi) and saved in JPG or PNG format.
 - c. Download the free Adobe Acrobat Reader DC
 - To download the free Adobe Acrobat Reader DC, go to this site: <https://get.adobe.com/reader/?promoid=KSWLH>
 - Before downloading the free Adobe Acrobat Reader DC application, make sure that all checkboxes in the “Optional Offers” section are clear or unchecked to avoid ads.
 - Next, click “Download Acrobat Reader” and follow instructions until the application is installed on computer.





2. Download Application Form via: <http://bit.ly/Deped-PNPKI>
 - a. Individually accomplish said form by clicking on text boxes. Please note that some items with either an asterisk (*) or “red-colored” boxes are required to be filled-out by the applicant/s.
 - b. After accomplishing the form, save it in this format:
LastName_FirstName_EmployeeNumber_[your affiliation]

Example: Bernas_Niña_EmployeeNumber_SDO

NOTE: PNPKI will not accept handwritten application forms.

3. Submission of Requirements - The submission of requirements will be within the DepEd LMS.
4. Notification from the Central Office, Regional or Division PNPKI Team, thru an advisory or memoranda, will be issued for updates and next steps.



OUAD00-0721-0169
To authenticate this document,
please scan the QR Code





Republic of the Philippines
Department of Education

NATIONAL CAPITAL REGION
SCHOOLS DIVISION OFFICE OF MUNTINLUPA CITY

Office of the Schools Division
Superintendent


JUL 19 2021

MEMORANDUM

**PREPARATORY ACTIVITIES ON THE IMPLEMENTATION OF DIGITAL
SIGNATURE**

To: OIC-Assistant Schools Division Superintendent
Chief Education Supervisor, Curriculum Implementation Division
Chief Education Supervisor, School Governance and Operations Division
Public Elementary/Secondary School Heads/OICs
All Others Concerned

1. Attached is a Memorandum from the Office of the City Election Officer on the above-mentioned title, contents of which are self-explanatory, for the information and guidance of all concerned.
2. Particular attention is invited to the third and fourth paragraphs of the said Memorandum, relative to the timeline and requirements for the application of the digital certificate.
3. For the **Procedure for the Application**, kindly refer to Sections 7, 8 and 9 Article IV of the Guidelines. To download the PNPKI Application Form for **Digital Certificate**, kindly use this link: https://bit.ly/PNPKI_Individual_Certificate_Application_Form_v2.
4. All Schools are enjoined to submit the summary of the names of teachers who applied for the Digital Signature on or before August 31, 2021 to Dr. Nerissa Roxas Lomeda, OIC- Assistant Schools Division Superintendent.
5. Immediate and wide dissemination of, and compliance to this Memorandum is desired.


DOMINICO C. IDANAN CESO V
Schools Division Superintendent

Enclosure: as stated
References: as stated
To be indicated in the Perpetual Index
under the following subjects:

SCHOOLS TEACHERS SERVICE COMMUNICATION

RRA/DM/**PREPARATORY ACTIVITIES ON THE IMPLEMENTATION OF DIGITAL SIGNATURE**
_____ / July 16, 2021



 Student Center for Life Skills Bldg., Centennial Ave, Brgy Tunasan,
Muntinlupa City
 (02) 805-9935, (02) 805 - 9940
 sdomuntinlupa@gmail.com



290 719 048



Office of the City Election Officer
Muntinlupa City
4th Level, Ayala Malls Southpark,
National Road, Alabang, Muntinlupa City

SDO-CITY OF MUNTINLUPA
Received _____
Date 7-14-21
Time 1:40pm

MEMORANDUM

TO : **Dr. DOMINICO C. IDANAN**
Schools Division Superintendent, Muntinlupa City

SUBJECT : **PREPARATORY ACTIVITIES ON THE IMPLEMENTATION OF
DIGITAL SIGNATURE**

DATE : 13 JULY 2021

Anent Memorandum dated 03 June 2021 entitled, "***Cascading of Information on Digital Signature to Department of Education***", the undersigned would like to respectfully forward a copy of **Comelec Guidelines on the Implementation of Digital Certificate for the 2022 National and Local Elections and Bangsamoro Autonomous Region of Muslim Mindanao¹** ("***Guidelines***", for brevity).

To reiterate, during the regular online meeting held on 20 January 2021, the Commission *En Banc* resolved that use of the digital signatures by the members of the Electoral Boards (EBs) and Board of Canvassers (BOC) will surely enhance the transparency and credibility of the elections. Hence, the implementation of the digital signature for use of the EBs and BOCs in the 2022 National and Local Elections.

Please note of the **timeline** provided under *Section 3, Article IV of the Guidelines*, to wit:

...the following schedule shall be observed in the filing and processing of applications for digital signatures:

Period	Applicants
August to September 2021	EB
October to November	BOC

Further, *Sections 4 and 5, Article IV of the same Guidelines* provides for the **requirements** which the applicants needed to prepare and to submit:

1. Duly accomplished application form;
2. Birth Certificate or Valid Philippine Passport;
3. Unified Multi-Purpose Identification Card. In absence, Any 2 government issued IDs;
4. 1 passport size ID picture;
5. Active mobile number; and
6. Active personal e-mail address

¹ Annex "A"

For the **Procedure for the Application**, kindly refer to *Sections 7, 8 and 9, Article IV of the Guidelines*. Furthermore, attached herewith is a hard copy of the PNPKI Application Form for Digital Certificate² and CD with soft copy of the PNPKI Application Form for Digital Certificate in PDF Format³.

For your information and guidance.


ATTY. KIMBERLEY JOY ALZATE-CU
Election Officer IV

² Annex "B"

³ Annex "C"



Republic of the Philippines
COMMISSION ON ELECTIONS
Intramuros, Manila

Office of Commissioner Marlon S. Casquejo
Steering Committee



MEMORANDUM

FOR : ALL REGIONAL ELECTION DIRECTORS

SUBJECT : POLICY GUIDELINES ON THE IMPLEMENTATION OF DIGITAL CERTIFICATES FOR THE 2022 NATIONAL AND LOCAL ELECTIONS AND BANGSAMORO AUTONOMOUS REGION OF MUSLIM MINDANAO ELECTIONS

DATE : 30 JUNE 2021

This has reference to the implementation of the digital signature for use of the Electoral Boards (EBs) in the 2022 National and Local Elections.

During the regular online meeting held on 16 December 2020, for purposes of preparatory activities for the 2022 National and Local Elections and in anticipation of the implementation of the use of the digital signatures by the EB and the possible deputation of the Field Officers as the Registration Authority, the Commission on Elections, in Minute Resolution No. 20-0591, approved the recommendation of the undersigned, as Steering Committee Head, the registration of the following personnel for their respective digital signatures with the Department of Information and Communications Technology (DICT), namely:

1. Regional Election Directors;
2. Assistant Regional Election Directors;
3. Provincial Election Supervisors; and
4. Election Officers.

Also on 20 January 2021, the Commission En Banc resolved, through Minute Resolution No. 21-0021, that the use of the digital signatures by the EB and Board of Canvassers (BOC) will surely enhance the transparency and credibility of the elections.

Since there is a need to provide guidelines, rules and regulations governing the application, approval, and revocation of the digital certificates to be used by the

NOTICE: All authorized recipients of any personal data information, privileged information and sensitive personal information contained in this document, including other pertinent documents attached thereto that are shared by the Commission on Elections in compliance with existing laws and rules, and in conformity with the Data Privacy Act of 2012 (R.A. No. 10173) and its Implementing Rules and Regulations, as well as the pertinent Circulars of the National Privacy Commission, are similarly bound to comply with said laws, rules and regulations, relating to data privacy, security, confidentiality, protection and accountability.

members of the EB and BOC in connection with the 09 May 2022 National and Local Elections and BARM election, attached is the policy guidelines to be observed during the implementation of the digital certificates.

For your guidance, implementation, and strict compliance.



Digitally signed
by Casquejo
Marlon Sabucido

MARLON S. CASQUEJO
*Steering Committee, Acting Head
Commissioner*

Cc: Executive Director Bartolome J. Sinocruz, Jr.
Deputy Executive Director for Operations Teopisto E. Elnas, Jr.
Director Divina E. Blas-Perez, Acting Director IV, EBAD
Director Jeannie V. Flororita, Director IV, ITD



Republic of the Philippines
COMMISSION ON ELECTIONS
Intramuros, Manila

**POLICY GUIDELINES ON THE IMPLEMENTATION OF DIGITAL CERTIFICATE FOR
THE 2022 NATIONAL AND LOCAL ELECTIONS
AND BANGSAMORO AUTONOMOUS REGION OF MUSLIM MINDANAO
ELECTIONS**

It is the policy of the State to ensure free, orderly, honest, peaceful, credible, gender responsive, socially inclusive, informed and COVID-19 free elections, and other similar electoral exercises by improving on the election process and adopting systems, which shall involve the use of an automated election system that will ensure the secrecy and sanctity of the ballots and all elections, consolidation and transmission of votes in order that the process shall be transparent and credible and that the results shall be fast, accurate, and reflective of the genuine will of the people.

During the regular online meeting held on 16 December 2020, for purposes of preparatory activities for the 2022 National and Local Elections and in anticipation of the implementation of the use of the digital signatures by the Electoral Board (EB) and Board of Canvassers (BOC) members, and the possible deputation of the Field Officers as the Registration Authority, the Commission on Elections, in Minute Resolution No. 20-0591, approved the recommendation of Commissioner Marlon S. Casquejo, as Steering Committee Head, the registration of the following personnel for their respective digital certificates with the Department of Information and Communications Technology (DICT), namely:

1. Regional Election Directors;
2. Assistant Regional Election Directors;
3. Provincial Election Supervisors; and
4. Election Officers.

Further, during the regular online meeting held on 20 January 2021, the Commission *En Banc* RESOLVED, through Minute Resolution No. 21-0021, that the use of the digital signatures by the EB and BOC will surely enhance the transparency and credibility of the elections.

This Policy Guidelines shall provide the rules and regulations governing the application, approval, and revocation of the digital certificates to be used by the members of the EB and BOC in connection with the 09 May 2022 National and Local Elections and BARMM elections.

ARTICLE I

GENERAL PROVISIONS

Section 1. *Coverage and Scope.* - These Guidelines shall apply to the procedures for the enrollment, approval, and revocation of the Digital Certificates that shall be used by the members of the EB and BOC in connection with the 09 May 2022 National and Local Elections and BARMM Elections.

ARTICLE II

DEFINITION OF TERMS

Section 1. *Definition of Terms.* - As used in these Guidelines:

- a) **APPLICANT** refers to an individual who is applying for a digital certificate with the Commission.
- b) **APPLICATION FORM** refers to the fillable Portable Document Format (PDF) application form for the issuance of the Philippine National Public Key Infrastructure (PNPKI) digital certificate.
- c) **BOARD OF CANVASSERS (BOC)** shall be composed of a Chairperson, Vice-Chairperson, and Member-Secretary for each province, city, municipality, district, and autonomous region.
- d) **CERTIFICATE AUTHORITY (CA)** is an entity that issues digital certificates.
- e) **DIGITAL CERTIFICATE** refers to a file issued by a Certificate Authority containing an individual's personal information as proof of the individual's (or machine's) electronic identity.
- f) **ELECTORAL BOARD (EB)** shall be composed of a Chairperson, a Poll Clerk, and a Third Member which shall be constituted and appointed by the Commission, through the Election Officer (EO), for every clustered or group precinct in the district, city, or municipality, in writing, in the form prescribed by the Commission.

- g) **ORS** refers to the Online Registration System, which shall be used by the Applicants in encoding their application for a digital certificate.
- h) **PNPKI** refers to the Philippine National Public Key Infrastructure.
- i) **RAO** refers to the Registration Authority Officer. There shall be two (2) RAOs. The RAO1 shall be the Election Officer of the city/municipality, whether holding a permanent appointment or in an acting capacity, who shall be in-charge in accepting all applications for digital certificate and documentary requirements as well as the encoding in the TMSRA.

The RAO2 shall be the Provincial Election Supervisor of the province, whether holding a permanent appointment or in an acting capacity, who shall be in-charge in approving all applications for digital certificates.

In the National Capital Region (NCR), however, the RAO1 shall be the Election Assistant of every city/municipality. The RAO2 shall be the Election Officer of every city/municipality.

- j) **RAA** refers to the Registration Authority Assistants, who shall be the Election Assistant of the city/municipality holding a permanent appointment outside NCR.
- k) **SUBSCRIBER** refers to a person who has been issued a digital certificate by the Commission.
- l) **TMSRA** refers Token Management System-Registration Authority, which shall be used by the RAOs in approving all applications for digital certificate.
- m) **VOTING CENTER** refers to the place or building where the polling place is located.

ARTICLE III

REGISTRATION AUTHORITIES

Section 1. *Functions and Responsibilities of the RAOs in the Application and Verification for Digital Certificates.* - There shall be one (1) RAO1 and one (1) RAO2 in every OEO.

- a) The RAO1 shall:
 - i. Accept and verify the Applicant's digital certificate application;

- ii. Conduct digitization and encoding of applications;
 - iii. Accept and verify Subscriber's request for revocation of digital certificate;
- b) The RAO2 shall:
- i. Approve certificate applications and requests for revocation.

In compliance with the Data Privacy Act, Plantilla Casuals, Job Orders, and LGU Casuals are prohibited from being designated as Registration Authorities.

Section 2. *Registration Authority Workflow.*

- a) The RAA receives and checks the completeness of the submitted documents and ensures that the same are readable;
- b) The RAO1 verifies, signs and seals application forms.
- c) The RAO1 encodes Applicant's data into the TMS Web Manager Add User.
- d) The RAO1 verifies the encoded data against the submitted application form.
- e) The RAO1 sends an email to the Applicant to schedule an online identity verification and validation of submitted documents.
- f) If Applicant's identity has been verified and all submitted documents have been validated, the RAO2 shall approve the application.
- g) Once approved, the RAO1 then sends an email notifying the Applicant that his/her digital certificate is ready for download.

ARTICLE IV

PERIOD, PROCEDURE AND REQUIREMENTS FOR THE APPLICATION AND APPROVAL OF THE DIGITAL CERTIFICATES

Section 1. *Who May Apply for a Digital Certificate that Shall be Used in Connection With the 09 May 2022 National and Local Elections and BARMM Elections* - All members of the EB and BOC who shall serve in the 2022 National and Local Elections and BARMM Elections shall be required to apply for their digital certificates.

Such members of the EB shall be public school teachers who are willing and available to render election service. Should there be a lack of public-school teachers willing, available or qualified to serve, the Commission may instead appoint the following persons, in this order of preference, in accordance with Section 3 of Republic Act No. 10756,¹ namely:

- a) Private school teachers;

¹ "An Act Rendering Election Service Non-Compulsory for Public School Teachers, Authorizing the Appointment of Other Qualified Citizens, Providing for Compensation and Other Benefits

- b) National government employees;
- c) Department of Education (DepEd) non-teaching personnel;
- d) Other national government officials and employees holding regular or permanent positions, excluding uniformed personnel of the Department of National Defense and all its attached agencies;
- e) Members of the Commission-accredited citizen arms or other civil society organizations and nongovernmental organizations duly accredited by the Commission; and
- f) Any registered voter of the city or municipality of known integrity and competence who is not connected with any candidate or political party.

The members of the BOC in each municipality, city, district, province, and in the Bangsamoro Autonomous Region in Muslim Mindanao (BARMM) shall be the following:

- a) **MBOC.** - The MBOC shall be composed of the Municipal Election Officer (Municipal EO) or a representative of the Commission, as Chairperson; the Municipal Treasurer, as Vice-Chairperson; and the District School Supervisor, or in the absence of the latter, the most senior Principal of the school district, duly designated as such by the District Supervisor as Member-Secretary.
- b) **DBOC for the Legislative District Taguig-Pateros.** - The DBOC for the legislative district of Taguig-Pateros shall be composed of the City EO or a lawyer of the Commission, as Chairperson; the City Prosecutor, as Vice-Chairperson; and the Schools Division Superintendent, as Member-Secretary.
- c) **CBOC.** - The CBOC shall be composed of the City Election Officer (City EO) or a lawyer of the Commission, as Chairperson; the City Prosecutor, as Vice-Chairperson; and the Schools Division Superintendent, as Member-Secretary. In cities within the National Capital Region (NCR) and other highly urbanized cities with more than one (1) City EO, the Regional Election Director (RED) shall designate the City EO who shall act as Chairperson. In cities which are outside the NCR and with more than one (1) City EO, the Provincial Election Supervisor (PES) shall designate the City EO who shall act as Chairperson.
- d) **PBOC.** - The PBOC shall be composed of the Provincial Election Supervisor (PES) or a lawyer of the Commission, as Chairperson; the Provincial Prosecutor, as Vice-Chairperson; and the Schools Division Superintendent, as Member-Secretary.
- e) **RBOC in the ARMM.** - The RBOC in the ARMM shall be composed of the Regional Election Director (RED) of the ARMM or a lawyer of the Commission, as Chairperson; a representative of equivalent rank from the

Department of Justice, as Vice-Chairperson; and a representative, likewise, of equivalent rank from the Department of Education, as Member-Secretary.

Section 2. *Substitute Members of the EB and BOC.* - Each city/municipality shall have a pool of substitute members for their respective EBs and BOCs who shall likewise enroll and be issued a digital certificate to enable them to serve in the 2022 National and Local Elections.

In case of the absence of the previously appointed EB and BOC on the day of the election and canvass, the following allocation shall be observed:

No. of Clustered Precincts in a VOTING CENTER	No. of Substitutes
Not more than 5 clusters	3
At least 10 clusters	5
At least 15 clusters	10
Over 15 clusters	15

Section 3. *Application Period.* - the following schedule shall be observed in the filing and processing of applications for digital certificates:

Period	Applicants
August to September 2021	EB
October to November 2021	BOC

Section 4. *Requirements.* - Applicants shall submit the following documents:

1. Duly accomplished application form;
2. Birth certificate or valid Philippine passport;
3. Unified Multi-Purpose Identification (UMID) compliant card. In the absence of a UMID-compliant card, ANY TWO (2) of government issued IDs;
4. One (1) passport size ID picture;
5. Active mobile number; and
6. Active personal e-mail address.

Section 5. *Document/s to be Submitted in Lieu of the Required Birth Certificate/Government Issued IDs.* - Should the Birth Certificate or any of the Government Issued IDs mentioned in the preceding section be unavailable at the time of the application, the Applicant may submit a Certification duly signed by the head of the department, agency, or office where he/she is currently employed, attesting the identity of the Applicant.

Section 6. *Application and Verification for Digital Certificates.* - All Applicants must:

- a) Submit clear scanned copies of requirements; and
- b) The Applicant must attend the online identity verification wherein they will present the original documents.

Section 7. *Procedure for the Application.* - The steps for online application are the following:

- a) Access the PNPKI website by entering <https://dict.gov.ph/pnpki-individual-certificate> in the web browser. Note that this page will also show the list of requirements;
- b) Click on "Application Form", download and open the application form using a PDF reader (i.e., Adobe or Foxit);
- c) Fill out all the required information in the form found in the red box;
- d) Fill out the Declaration page – the date, place, and name of Applicant in Page 2. It will automatically fill out Page 4. Once complete, save the file as PDF and print;
- e) Send the application form and requirements enumerated in Section 3 of this Article to the OEO's official email;
- f) The RAA will check the completeness of the information and submitted requirements;
- g) If complete, the RAO1 will send an email to the Applicant to schedule a video call session for identity verification and validation of submitted documents. The said email shall contain the following information:
 - i. Date and Time of the Online Identity Verification;
 - ii. Video call platform; and
 - iii. Video call credentials;
- h) During the video call session with the RAO1, the Applicant shall sign Pages 2 and 4 of the application forms and submit the same to the OEO's official email;
- i) Once received and approved by the RAO2, the Applicant shall receive his/her digital certificate download credentials through email.

In downloading their digital certificates, Applicants are discouraged from using public or shared computers. Please note that documents may only be signed digitally using laptops and desktops installed with Windows or Mac Operating System.

Section 8. *Online Identity Verification of Applicants.* - In relation to subparagraph (g) of the immediately preceding section, the following guidelines must be observed:

- a) Identity verification shall be done online through video call supported platforms that are free of charge, including, but not limited to, Skype, Viber, Webex, and Zoom;
- b) The video call session shall be scheduled and facilitated by the RAO1 in a manner that will not disrupt the continuing registration of voters;
- c) During the video call session, Applicants must present the original copies of their submitted documents and IDs. The RAA shall take a picture of the Applicant while holding the original document for verification and documentation.

Section 9. *Face-to-Face Verification/Exception to the Online Identity Verification of Applicants.* - In cities/municipalities where internet connection is unavailable or unstable, the RAA shall contact the Applicants through their registered working mobile number to inform them of their scheduled appointment at the OEO.

The personal identity verification shall be scheduled in a manner that will not disrupt the ongoing voters registration.

ARTICLE V

ISSUANCE OF DIGITAL CERTIFICATES

Section 1. *PNPKI Self-Service Portal for Enrollment, Installation, and Downloading of Duly Approved PNPKI Digital Certificate.* - Once the PNPKI digital certificate is approved, the RAO1 shall send an email notification to the Subscriber with instructions to enroll, download, and install his/her digital certificate in the PNPKI Self-Service Portal.

The certificate shall be deemed issued and accepted once the digital certificate has been downloaded and accessed. Therefore, upon enrollment in the PNPKI Self-Service Portal, the Subscriber must review the contents of his/her digital certificate before downloading. Subscriber may object to the certificate or its contents and request for corrections within five (5) days from the issuance thereof.

Beyond the five (5) day period, corrections will no longer be allowed. The Subscriber must then apply for the revocation of the rejected digital certificate and issuance of a new certificate.

Section 2. *Subscriber's Responsibility over the Digital Certificate.* - Once the digital certificate has been accepted, the Subscriber shall be responsible for the custody and proper use thereof in a safe and secure manner.

Section 3. *Validity of the Digital Certificate.* - the issued digital certificate will only be valid for two (2) years from issuance thereof.

ARTICLE VI

REVOCATION OF DIGITAL CERTIFICATES

Section 1. *Revocation of the Digital Certificate.* - The digital certificate duly issued to the members of the EB, BOC, and their substitutes may be revoked in case of the following:

- a) Key compromise - the Subscriber's private key was compromised;
- b) CA compromise - the key of the Certificate Authority was compromised;
- c) Superseded - the Subscriber has a new certificate;
- d) Undisclosed - the Subscriber did not state the grounds for his/her application for revocation;

ARTICLE VII

MISCELLANEOUS PROVISIONS

Section 1. *Reporting and Records Keeping.* - the Election and Barangay Affairs Department (EBAD) shall provide the template of the report on the implementation of this Resolution. EBAD shall likewise submit monthly reports on the progress of the accepted applications and actions taken thereon to the Project Management Office and Steering Committee for the 2022 National and Local Elections and BARMM Elections.

Section 2. *Roles of the Regional Election Directors (REDs), Assistant Regional Election Directors (AREDs), Provincial Election Supervisors (PESs) and Election Officers (EOs).* - The REDs, AREDs, PESs, and EOs shall ensure the strict implementation of the provisions of this Guideline and the timely compliance with the reportorial requirements.

APPROVED



PHILIPPINE NATIONAL PKI

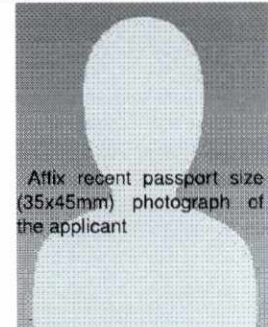
APPLICATION FOR DIGITAL CERTIFICATE

Application ID Number (For Official Use only)

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Instructions:

1. Please fill the form in BLOCK LETTERS ONLY.
2. Required fields are marked with an asterisk (*).
3. Present one (1) copy and the original documents to our Registration Authority for verification and attestation.
4. Any information that is not verified shall not be included in certificates.
5. Any discrepancy or inconsistency in the form will lead to delay and/or rejection.



Affix recent passport size (35x45mm) photograph of the applicant

1. CERTIFICATE CLASS		2. CERTIFICATE TYPE		3. METHOD OF ACTIVATION	
1A Individual		2A Signing		3A USB Token	
		2B Authentication		3B Online Download	

4. APPLICANT'S DETAILS							
4A* Last Name		4B* First Name		4C* Middle Name		4D* Name Extension (JR/SR/III)	
4E* Gender	Male Female	4F* Nationality		4G* Date of Birth (DD/MM/YYYY)			
4H* TIN			4I SSS No.				
4J GSIS No.		4K Philhealth No.		4L Pag-ibig No.			
4M CRN No.			4N Other IDs presented during face to face verification				
4O* Organization / Agency / Company							
4P* Organizational Unit / Department / Division							
4Q Marital Status	Single Married Widow						
4R Employment Status	Working Student Self-employed Unemployed Senior Citizen						
	Last Name	First Name	Middle Name	Name Extension (JR/SR/III)	Birthdate (DD/MM/YYYY)	Living / Deceased	
4S Spouse Name							
4T Mother's Maiden Name							
4U Father's Name							

5. CONTACT DETAILS			
Residential Address			
5A* Unit/Room/House No.		5B* Street	
5C* Barangay		5D* Municipality/City	
5E* Province		5F* Zip Code	
5G Landline No.		5H* Mobile No.	
5I* Email Address		5J Alternate Email Address	
Office Address			
5K Unit/Room/Floor No.		5L Building	
5M Street		5N Barangay	
5O Municipality/City		5P Province	
5Q Zip Code		5R Landline No.	
5S Email Address		5T Fax No.	

PNPKI RA Form 2018-01A
Date Revised February 2020



6. DECLARATION

I hereby agree that I have read and understood the provisions of the Subscriber's Agreement; that all information provided and documents submitted in relation to this application is true and correct to the best of my knowledge; that I am duly authorized to make this application; that I consent to the subscriber agreement and will abide by the same; that I accept the publication of my certificate information.

I authorize and expressly give consent to the National PKI through its authorized representative(s) to verify my personal information from whatever source it deems appropriate.

Date: Place: Name of Applicant:

Signature:

7. CHECKLIST OF DOCUMENTS TO BE SUBMITTED ALONG WITH THE APPLICATION

Present the ff. original documents with photocopy to our Registration Authority for verification and attestation

Required Documents:

Birth certificate issued by PSA **OR** valid Passport
Alien Certificate of Registration (ACR) card for foreigners
Unified Multi-purpose Identification Card (UMID) Compliant Card

In the absence of UMID-compliant card, any two (2) of the following cards are allowed as valid ID's

Driver's License
Professional Regulation Commission (PRC) ID
National Bureau of Investigation (NBI) Clearance
Postal ID
Voter's ID
Government Service Insurance System (GSIS) e-Card
Government Office and GOCC ID, e.g. Armed Forces of the Philippines (AFP ID), Home Development Mutual Fund (HDMF)
Social Security System (SSS) Card
Senior Citizen Card
Overseas Workers Welfare Administration (OWWA) ID
OFW ID
Integrated Bar Of The Philippines ID
Department of Social Welfare and Development (DSWD) Certification
Company IDs Issued by Private Entities or Institutions Registered with or Supervised or Regulated either by the BSP, SEC, or IC

8. DISCLAIMER

The collected personal information is utilized solely for documentation and processing purposes within the DICT and is not shared with any outside parties, in accordance with the Data Privacy Act of 2012.

TO BE FILLED BY RA OFFICE ONLY

I declare that the applicant has provided correct information in this application form. I have checked and verified the application form and supporting documents.

RA Code: Name:
Signature:
Date: Place:

RA Seal and
Stamp



THIS FORM IS NOT FOR SALE



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.
- f) 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 CRLs 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/.

Date: Place: Name of Applicant:

Signature: _____

(Please sign in the presence of an administering officer)

