



Republic of the Philippines
OFFICE OF THE SECRETARY
Elliptical Road, Diliman
1100 Quezon City

MEMORANDUM ORDER

No. 10

Series of 2022

SUBJECT : GUIDELINES ON THE USE OF DIGITAL SIGNATURE IN THE DEPARTMENT OF AGRICULTURE

I. RATIONALE

This Memorandum Order (MO) shall prescribe guidelines on the use of digital signatures to electronic documents, and provide rules and controls including duties and responsibilities of the concerned offices and signing officials/employees in the Department of Agriculture (DA).

Through digitalization, electronic documents shall be recognized, along with digital signatures, as valid documents following existing laws, rules, and regulations on the matter. Moreover, controls should be implemented to ensure authentication of documents, non-repudiation of the signatures, and integrity of the documents signed.

II. LEGAL BASES

1. Republic Act (RA) No. 8792 or Electronic Commerce Act provides the recognition and use of electronic commercial and non-commercial transactions and documents.
2. Section 9(e) of RA No. 11032 or Ease of Doing Business requires that all government agencies covered by this RA shall, when applicable, develop electronic versions of licenses, clearances, permits, certifications or authorizations with the same level of authority as that of the signed hard copy.
3. Government Procurement Policy Board (GPPB) Resolution No. 16-2019 approves the use of digital signature in procurement-related documents.
4. Data Privacy Act of 2012 and the Cybercrime Prevention Act of 2012 requires that government agencies shall establish and implement controls and secure means of providing electronic services to the public.
5. Commission on Audit (COA) Circular 2021-006 dated September 6, 2021 provides Guidelines in the use of Electronic Documents, Electronic Signatures, and Digital Signatures in government transactions following the existing laws, rules, and regulations.

A food-secure and resilient Philippines

with empowered and prosperous farmers and fisherfolk



III. SCOPE

This MO shall apply in the event that the DA officials and employees issue electronic documents in lieu of paper documents, where the signature of an authorized signatory is required. Nothing in the MO shall be construed as prohibiting an office from submitting paper documents, or a combination of paper and electronic documents.

It shall cover the following DA offices: Central Office, Regional Field Offices (RFOs), Bureaus, Attached Agencies and Corporations, Banner Programs, Locally-funded and Foreign-assisted projects.

IV. DEFINITION OF TERMS

1. Certificate Authority (CA) - refers to a trusted entity that manages and issues security certificates and public keys that are used to secure communications in a public network or the internet. The Department of Information and Communications Technology (DICT) is the authorized Certificate Authority in the government.
2. Digital Certificate - is a file issued by a CA or the DICT - Philippine National Public Key Infrastructure containing the user's personal information just like an ordinary ID, only in this case, it is digital. It is used to encrypt, authenticate or digitally sign a document sent through email.
3. Digital Signature - refers to a secure type of electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine:
 - a. Whether the transformation was created using the private key that corresponds to the signer's public key; and
 - b. Whether the initial electronic document had been altered after the transformation was made.
4. Electronic Document - refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.
5. Public Key Infrastructure (PKI) - is an infrastructure that secures communications among individuals and government entities. This way, the government's delivery of services to citizens and businesses becomes safer.

A food-secure and resilient Philippines

with empowered and prosperous farmers and fisherfolk



V. GUIDELINES

DA officials/employees who are signatories of official documents shall apply for a digital signature certificates at the DICT through the Information Communications Technology Service (ICTS) of DA Central Office (DA-CO), or its equivalent offices in DA's attached offices and submit the documentary requirements listed in Annex "A" of this MO.

1. Electronic documents must be processed in a secured computer and network system that complies with the DA prescribed cybersecurity policies.
2. The document to be signed digitally must be unalterable, in PDF format, and final version after clearances from concerned signatory.
3. Since digital signatures are electronic files that can be stored in storage devices such as office computers, flash drives or any cloud storage, the owner must take responsibility for its usage and storage. It is assumed that nobody will share his/her signature and password. Hence, improper use of digital signature may be subjected to applicable administrative penalties provided by the Data Privacy Act of 2012 and or Electronic Commerce Act whichever is applicable.
4. The use of PNPKI digital signature will be accepted in lieu of wet signatures on the following documents:
 - a. Correspondences within DA offices, especially during this pandemic, where Work from Home (WFH) is being implemented as an alternative work arrangement.
 - b. Other DA documents as identified:
 - Administrative Documents such as Memorandum, Leave Application Forms, Daily Time Record, Accomplishment Report;
 - Financial Documents such as eNGAS-generated electronic reports (from Accounting System and e-Budget System); Signatures in the document may be in combination of digital and wet signature.

However, the use of digitally signed documents as attachments for financial transactions would require proper authentication, since printouts of documents are considered as duplicates or secondary copies, and shall have a notation (footer) or disclosure "The original of this document is in digital format" or other similar language.

- Financial electronic documents should be processed under the same office as that of the first authorized signatory:

Ex.1. Financial Statements (FS)/Journal Entry Vouchers (JEVs)/Tax Remittances are to be processed under the supervision of the Chief Accountant.

Ex.2 Payrolls are to be processed under the supervision of the Chief of the Personnel Division.

A food-secure and resilient Philippines

with empowered and prosperous farmers and fisherfolk



Ex.3 Obligation Request Status (ORS) are to be processed under the supervision of the Chief of the Requesting Unit. Performance monitoring documents such as Individual Performance Commitment and Review (IPCR), Office Performance Commitment and Review Form (OPCR), Service Performance Commitment Review (SPCR) and other accomplishment reports;

- c. Procurement related documents defined in the Government Procurement Policy Board Resolution No. 16-2019 may be processed and signed using PNPKI, including but not limited to:
- Project Procurement Management Plan;
 - Annual Procurement Plan;
 - Invitation to Bid;
 - Request for Expression of Interest;
 - Supplemental / Bid Bulletin;
 - Notice of Postponement of Bid Opening;
 - Notice of Eligibility or Ineligibility;
 - Notice of Short Listing;
 - Abstract of Quotations;
 - Abstract of Bids as Read;
 - Abstract of Bids as Calculated;
 - Bid Evaluation Report;
 - Notice to Bidder with the Lowest Calculated Bid;
 - Post-Qualification Report;
 - Notice of Post-disqualification;
 - Reply to Motion for Reconsideration and Protest;
 - Blacklisting Order;
 - Procurement Monitoring Report;
 - Agency Procurement Compliance and Performance Indicators; and
 - Memorandum from the Procurement Office to concerned parties
- d. Government permits and licenses, provided there is compliance with the requirements as set forth in the Electronic Commerce Act or RA No. 8792; and
- e. Electronic documents intended for external communications may be signed using PNPKI digital signature;

A food-secure and resilient Philippines
with empowered and prosperous farmers and fisherfolk



5. The DA Contract of Service (COS) personnel will be allowed to use digital signature only on the following documents:


- a. Daily Time Record (DTR);
- b. Accomplishment Report (AR);
- c. Job Completion/ Satisfaction Certification;
- d. Travel reports; and
- e. Other documents that may be allowed by law.*

*Other documents needs approval/notation from the immediate supervisor (holder of a plantilla position)

6. Prescribed Format. The following in a human-readable form shall accompany the digital signatures:


- a. For memo, communication and other documents: Full name of the signatory with the date and an image of the signatory's handwritten signature;

For guidance, an example of a properly formatted digital signature is shown below:

 Digitally signed
by Juan Dela
Cruz
Date: 2020.05.21


- b. For financial and procurement related documents: Full name of the signatory with the date & timestamp, and an image of the signatory's handwritten signature;

For guidance, an example of a properly formatted digital signature is shown below:

 Digitally signed
by Juan Dela
Cruz
Date: 2020.05.21
19:37:33 +08'00'

- c. For authorized employees who are required to conduct prior review before the signatories may use smaller images as their initials: Full name of the signatory with date and an image of the signatory's handwritten signature;

For guidance, an example of a properly formatted initials is shown below:

 Digitally signed
by Juan Dela
Cruz
Date: 2020.05.21

A food-secure and resilient Philippines

with empowered and prosperous farmers and fisherfolk



VI. STATEMENT OF DUTIES AND RESPONSIBILITIES

For consistency, a DA Official/Employee or an authorized signatory who owns a digital signature should consistently use such digital signature in all electronic documents as prescribed in the Section V of this MO.

1. DA officials/employees who own a digital signature shall use and store their respective digital signature responsibly and in accordance with this MO. A digital signature is still vulnerable to forgery or misuse. It must be used responsibly as it represents one's identity.
2. DA shall formulate and develop data protection and cybersecurity policies to promote safe digital transactions.
3. The following are duties and responsibilities of a Digital Signature Holder, ICTS of DA-CO, and ICT Units of the DA's attached offices.

a. Digital Signature Holder

- i. Prepare and submit the application form and mandatory requirements to the Cybersecurity Bureau - Digital Certificate Division of the DICT or online at <https://sites.google.com/dict.gov.hk/pnpki/ors> through ICTS or its equivalent offices in the DA's attach offices.
- ii. Attend the scheduled interview by the DICT;
- iii. Download and install of the digital certificates; and
- iv. Install Adobe Acrobat Reader and other software required in using the digital signature.

b. Information and Communications Technology Service (ICTS) of DA Central Office

- i. Assist the DA officials/employees in its application for digital signature certificates at the DICT under PNPKI;
- ii. Coordinate with the Cybersecurity Bureau - Digital Certificate Division of the DICT;
- iii. Conduct trainings or orientation to disseminate information on the use of digital signature;
- iv. Assist DA employees in the downloading and installation of the digital signatures;
- v. Develop a system and provide a secure storage for electronically signed documents including supporting documents for financial transactions;
- vi. Answer queries and concerns related to the application, download, installation, and use of digital certificates;
- vii. Monitor status of DA digital signature applicants and users; and
- viii. Provide other technical assistance.

A food-secure and resilient Philippines

with empowered and prosperous farmers and fisherfolk



c. ICT Units of the DA RFOs, Bureaus, Attached Agencies and Corporations, Banner Programs, Locally-funded and Foreign-funded project

- i. Assist the DA officials/employees/COS in its application for digital signature certificates at the DICT under PNPKI;
- ii. Coordinate with the ICTS of the DA-CO;
- iii. Facilitate the enrollment of their respective offices;
- iv. Assist employees in their respective offices in the downloading and installation of the digital signatures;
- v. Answer queries and concerns related to the application, downloading installation, and use of digital certificates;
- vi. Monitor the status of application in their respective offices and submit reports to ICTS of the DA-CO through ictpsd@da.gov.ph; and
- vii. Provide other technical assistance.

VII. LIMITATIONS

1. COS personnel shall not be authorized as signatories of official and financial documents such as attachments to Disbursement Vouchers, among others.
2. COS personnel can process electronic documents but the signatory should be a regular-plantilla position holder.
3. The use of digital signature shall not apply on documents for notarization.

VIII. EFFECTIVITY

These guidelines shall take effect immediately and shall remain in force until revoked or superseded by later issuances.

Done this 9th day of February 2022.



WILLIAM D. DAR, Ph.D.

Secretary

DEPARTMENT OF AGRICULTURE

In replying pls cite this code :
For Signature: S-01-22-0452
Received : 01/28/2022 01:49 PM

A food-secure and resilient Philippines

with empowered and prosperous farmers and fisherfolk



Annex A. DOCUMENTARY REQUIREMENTS:

1. Unified Multi-purpose Identification (UMID) compliant card (Photocopy)
2. Birth Certificate or valid Philippine Passport (Photocopy)
3. Passport size ID picture

* In the absence of UMID-compliant card, ANY TWO of the following cards are allowed as valid IDs based on Banko Sentral ng Pilipinas (BSP) Circular No, 608 series of 2008:

- o Passport
- o Driver's License
- o Professional Regulation Commission (PRC) ID
- o Police Clearance
- o Postal ID
- o Voter's ID
- o Government Service Insurance System (GSIS) e-Card
- o Social Security System (SSS) Card
- o Senior Citizen Card
- o Overseas Workers Welfare Administration (OWWA) ID
- o OFW ID
- o Seaman's Book
- o Alien Certification of Registration / Immigrant Certificate of Registration
- o Government Office and GOCC ID, e.g. Armed Forces of the Philippines (AFP ID), Home Development Mutual Fund (HDMF ID)
- o Certification from the National Council for the Welfare of Disabled Persons (NCWDP)
- o Department of Social Welfare and Development (DSWD) Certification
- o Integrated Bar of the Philippines ID
- o Company IDs Issued by Private Entities or Institutions Registered with or Supervised or Regulated either by the BSP, SEC or IC
- o Taxpayer Identification Number (TIN)
- o Phone number (mobile and / or landline)
- o Email address owned by the individual or authorized by the owner for use by the subscriber; and
- o Consent to verify and share the information submitted.

A food-secure and resilient Philippines
with empowered and prosperous farmers and fisherfolk

