



DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES  
KAGAWARAN NG KAPALIGIRAN AT LIKAS NA YAMAN



NOTICE OF MEETING

FOR : Representatives (1 per Office)  
Office of the Undersecretaries  
Office of the Assistant Secretaries  
Office of the Service Directors  
Environmental Law Enforcement and Protection Service  
River Basin Control Office (RBCO)  
Manila Bay Coordinating Office (MBCO)  
Comprehensive Agrarian Reform – National Coordinating Office (CARP-NCO)  
Pasig River Coordinating and Management Office  
Legislative Liaison Office  
Document Management and Operations Support  
Indigenous Peoples Concerns – Mindanao and Bangsamoro Autonomous Region in Muslim Mindanao Affairs  
Strategy Management and Organizational Transformation  
  
All Division Chiefs (1 Representative per Division)

FROM : The OIC Director  
Financial and Management Service

DATE/TIME : May 2, 2024 (Thursday) / 9:00 a.m.

VENUE : *Via Zoom Conference*  
**Zoom Link: <https://bit.ly/ConsultationEDADSBatch1>**  
**Meeting ID: 930 8530 7854**  
**Passcode: DENRFMS**

AGENDA :

1. Online Consultation on the Proposed Internal Guidelines on the Use of Electronic Documents and Digital Signatures in DENR (Batch 1); and
2. Other matters.

Your attendance is highly enjoined.

IMELDA R. DELA CRUZ

MEMO NO. 2024 - 372

Visayas Avenue, Diliman, Quezon City 1100, Philippines  
[www.denr.gov.ph](http://www.denr.gov.ph)



Republic of the Philippines  
**COMMISSION ON AUDIT**  
Commonwealth Avenue, Quezon City, Philippines

CIRCULAR

No. : 2021-006  
Date: SEP 06 2021

TO : All Heads of Departments, Bureaus, Offices, Agencies and Instrumentalities of the National Government, Heads of the Local Government Units, Managing Heads of Government-Owned and/or Controlled Corporations, Chiefs of Financial and Management Services, Chief Accountants, Cashiers, Disbursing Officers, and Budget Officers; Assistant Commissioners, Directors and State Auditors of the Commission on Audit (COA); and All Others Concerned

SUBJECT : Guidelines on the use of Electronic Documents, Electronic Signatures, and Digital Signatures in Government Transactions

**I. RATIONALE**

The Philippine Constitution provides that the State recognizes the vital role of communication and information in nation-building. It shall regulate the transfer and promote the adaptation of technology for the national benefit.

Republic Act No. 8792 or the Electronic Commerce Act of 2000<sup>1</sup> provides for the legal recognition of electronic signatures and imposes strict requirements before an electronic signature qualifies as a handwritten signature. The same law allows electronic transactions in government and allows appropriate government entities to adopt and promulgate rules, regulations, or guidelines to specify the use of an electronic signature, the type of electronic signature required, the manner the electronic signature shall be affixed to the electronic data message or electronic document, and the control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic data messages or electronic documents or records of payments.

The Supreme Court also recognizes the use of electronic signatures in its Rules on Electronic Evidences which provides that an electronic signature or digital signature authenticated in the manner prescribed is admissible in evidence as the functional equivalent of the signature of a person on a written document.

---

<sup>1</sup> An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use Thereof and for Other Purposes.

The same rule gives disputable presumption to electronic signature in favor of its validity after its authentication.

To promote the growth and wide use of e-government services and address the authentication, integrity and non-repudiation concerns, Executive Order No. 810 was issued in 2009 to institutionalize the National Certification Scheme for Digital Signatures in the country and designate the National Computer Center (NCC) under the Commission on Information and Communications Technology, now Department of Information and Communications Technology (DICT), as the Government Certificate Authority to provide the necessary services in implementing the scheme. This paved the way for DICT's Philippine National Public Key Infrastructure (PKI) [DICT-PNPKI] service which enables the widespread use of digital signatures nationwide. The DICT-PNPKI makes use of the PKI framework – a robust system that uses paired keys to provide security and authentication for electronic information transfers. Relative thereto, COA Memorandum 2009-073 dated July 23, 2009 was issued to require state auditors to ensure that their audited agencies providing electronic services to their clients are/will be implementing the use of digital signature in their respective e-government services.

The Government Procurement Policy Board (GPPB) in its Resolution No. 16-2019 allowed and approved the use of digital signature in all GPPB issuances and in procurement related documents. Similarly, the Bureau of Internal Revenue (BIR) issued Revenue Memorandum Circular No. 29-2021 which allows the use of electronic signatures on BIR Forms 2304, 2306, 2307 and 2316. The Anti-Red Tape Authority intensifies its drive to streamline the processes in all government entities and take advantage of technology, especially in the event of a disaster or any state of emergency such as the COVID-19 pandemic as it allows government officials to approve transactions and make payments without necessarily being physically present. Furthermore, COA Circular No. 2004-006 dated September 9, 2004 implies admissibility of digitally-signed documents in audit.

Lastly, the enactment of the Data Privacy Act of 2012<sup>2</sup> and the Cybercrime Prevention Act of 2012<sup>3</sup> requires that government agencies establish and implement controls and secure means of providing electronic services to the public. Digital signatures, by design, contribute significantly to these control requirements.

Therefore, this Circular shall prescribe guidance on the use of electronic signatures for accountability purposes to resolve doubts over the reliability of information to be used as audit evidence.

---

<sup>2</sup> An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes, Republic Act No. 10173, August 15, 2012.

<sup>3</sup> An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes, Republic Act No. 10175, September 12, 2012.

## II. SCOPE AND COVERAGE

This Circular shall apply when the audited agency submits electronic documents to the auditor in lieu of paper documents, where the signature of an authorized signatory is required. Nothing in the Circular shall be construed as prohibiting an audited agency from submitting paper documents, or a combination of paper and electronic documents.

## III. DEFINITION OF TERMS

- a. **Asymmetric or public cryptosystem**, more commonly referred to as public key infrastructure, means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key for verifying the digital signature.<sup>4</sup>
- b. **Certificate Authority (CA)** refers to a trusted entity that manages and issues security certificates and public keys that are used for secure communication in a public network or the internet. The DICT is the authorized Certificate Authority in the government.
- c. **Digital Certificate** is a file issued by a CA or the DICT-PNPKE 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 an email and document.
- d. **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:
  - i. whether the transformation was created using the private key that corresponds to the signer's public key; and
  - ii. whether the initial electronic document had been altered after the transformation was made.<sup>5</sup>
- e. **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.<sup>6</sup>

<sup>4</sup> Rules on Electronic Evidence, A.M. No. 01-7-01-SC, July 17, 2001, Rule 2, Section 1(a).

<sup>5</sup> Rules on Electronic Evidence, Rule 2, Section 1(e).

<sup>6</sup> Rules on Electronic Evidence, Rule 2, Section 1(h).

- f. **Electronic Signature** refers to any distinctive mark, characteristic and/or sound in electronic form, secured and non-secured, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.<sup>7</sup> For purposes of this Circular, electronic signature refers not only to the handwritten signatures, but the whole process adopted in approving an electronic data message or electronic document. Examples of electronic signatures include: a scanned image of the person's ink signature, a mouse squiggle on a screen or a hand-signature created on a tablet using the person's finger or stylus, a signature at the bottom of the email, a typed name, a biometric hand-signature signed on a specialized signing hardware device, a video signature, a voice signature, etc.<sup>8</sup>
- g. **Key Pair** refers to the two mathematically related keys, the public and private keys. Whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa. Public and private keys are paired for secure communication, such as email.
- h. **Private Key** is a bit of code that is paired with a public key to set off algorithms for text encryption and decryption. It is created as part of public key cryptography during asymmetric-key encryption and used to decrypt and transform a message to a readable format. A private key is also known as a secret key.
- i. **Public Key** is also a bit of code used to encrypt data. The key is provided by the CA and is made available to everyone through a directory or email.
- j. **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, faster and more efficient.

#### IV. GUIDELINES

##### A. General Principles and Guidelines

- 1. Submission of electronic documents with electronic signatures (including digital signatures) following the rules in this Circular, shall mean sufficient compliance to the requirement of submission of duly signed document as any other duly signed paper document used in government transactions.

---

<sup>7</sup> Rules on Electronic Evidence, Rule 2, Section 1(j).

<sup>8</sup> Dave Venance. What is an e-Signature? Part 1. *available at* [https://www.4point.com/blog/2017/06/what\\_is\\_an\\_e-signatu.html](https://www.4point.com/blog/2017/06/what_is_an_e-signatu.html) (last accessed: June 20, 2020).

2. When under existing rules a document requires a signature, the use of electronic signature (including digital signature) on the electronic document shall be an accepted alternative and shall be equivalent to the signature of a person on a written document such as, but not limited to, procurement-related documents, Disbursement Vouchers, Requisition and Issuance Slips, Purchase Orders, Contracts, and Memoranda among others.
3. Private parties involved in transactions with government, in the absence of a digital certificate, may use other types of electronic signature, subject to the controls implemented by the transacting government entity.

**B. Management Responsibility in using Electronic Documents**

4. All government entities that elect to use and/or implement a system using digital signature or other types of electronic signature on electronic documents under this Circular shall issue internal rules in the adoption of the same, including sanction for unauthorized and illegal use of digital certificates or electronic signatures, subject to existing laws and regulations such as the Cybercrime Prevention Act of 2012, as well as to rules of the DICT. They shall submit a Management Representation or Policy Statement on the use of signature on electronic documents in their operations to their respective Auditors, together with the approved internal rules. A sample form of the Management Representation is attached as Annex A.
5. To secure the electronic records with signatures, the government entity shall:
  - a. Designate a focal person for all matters pertaining to electronic signing implementation of the government entity;
  - b. Develop, maintain, and update accordingly the system documentation used for creating electronic records with signatures;
  - c. Develop, maintain and implement standard operating procedures for the creation, utilization, storage, security, and management of electronic records that contain signatures, to ensure that the records are protected from unauthorized alteration or destruction;
  - d. Implement a security awareness program such as training the employees on the acceptable use of signature on electronic documents; and
  - e. Develop and implement policy and guidelines on the following:
    - Scope of the employee's authority to use signature on electronic documents
    - Security measures for the protection of digital certificate, if any
    - Sanctions for misuse or abuse of signatures.

4

4

### C. Specific Guidelines on the use of Digital Signatures

6. All officials and employees designated/authorized to sign documents using digital signature shall apply for their individual certificates with the DICT as the Government Certificate Authority through its PNPKI service where they shall undergo a process of identity verification and be oriented on the proper and sound use of digital certificates as prescribed under the DICT-PNPKI Digital Certificate Subscriber Agreement. Alternatively, they may apply for their individual certificates from any other CA accredited or recognized by the Department of Trade and Industry – Philippine Accreditation Bureau (DTI-PAB) to issue digital certificates to be used in government transactions.<sup>9</sup>
7. At a minimum, the implementation of digital signatures shall bear the following characteristics:
  - a. Authentication – linking the signatory to the information;
  - b. Integrity – assuring that the document has not been altered during transmission; and
  - c. Non-repudiation – ensuring that the signer of the electronic document cannot at a later time deny having signed it.
8. Government entities shall have the duty to inform COA Auditors, in case of revocation or expiration (without renewal) of the digital certificate. They shall keep updated records of Certificate Revocation List, which contains list of certificates that would have been compromised or are expired so that the government entity knows which digital certificates are no longer valid or have been revoked by the CA.
9. To ensure verifiability of digitally-signed documents, the same shall be maintained in its original form and submitted electronically. For this purpose, print-out of documents are considered 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.
10. In signing an electronic document, a government official or the designated signatory shall express in unequivocal terms his/her intent or purpose for signing through a notation close to his/her signature or through a footnote. However, such notation or footnote is not required when the intent is clear as appearing in the document.
11. When using digital signature, electronic document is preferred to be in Portable Document Format (pdf), Microsoft Excel Document (xlsx), or combination of both. Any other compatible format may also be used, provided it allows secure implementation of digital signature. For digitally

---

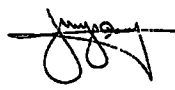
<sup>9</sup> Executive Order No. 810, June 15, 2009, Section 3(d).

signed e-mails, it is recommended that a government domain email be used (e.g. name@agency.gov.ph)

12. When a digital certificate is to be used to sign a document, the same should be valid, unexpired, and unrevoked at the time of signing.
13. The following details in a human-readable form, shall accompany the digital signatures:
  - a. Full name of the signatory; and
  - b. 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 DelaCruz  
Date: 2020.05.21  
19:37:33 +08'00'



However, other formats shall be acceptable so long as they clearly display items a and b above.

14. It is the duty of every certificate subscriber to give notification to the designated focal person mentioned in Item 5 and to the concerned auditor for revocation when he/she suspects that his/her certificate has been compromised.
  15. The document should be protected after all signatories had affixed their digital and other types of electronic signatures to ensure that the document will not be altered thereafter.
- D. Specific Guidelines on the use of Electronic Signature (other than Digital Signature)**

16. When the officer opts to use an electronic signature other than a digital signature on an electronic document, the signed electronic document may be validly accepted provided the agency is able to establish that:
  - a. the electronic signature is that of the person to whom it correlates;
  - b. the electronic signature was affixed by that person with the intention of authenticating or approving the electronic document to which it is related or to indicate such person's consent to the transaction embodied therein;
  - c. the methods or processes utilized to affix or verify the electronic signature, if any, operated without error or fault; and



- d. the person whose e-signature was affixed, takes responsibility and assumed accountability that the document remained unchanged until it was submitted to the auditor.

**V. SAVING CLAUSE**

Cases not covered in this Circular shall be referred to the Systems and Technical Services Sector, this Commission, for resolution.

**VI. SUPPLEMENTARY APPLICATION OF THE RULES OF COURT AND OTHER LAWS**

This Circular shall primarily govern the use of digital and other types of electronic signatures in government transactions under the audit jurisdiction of COA, in accordance with the E-Commerce Act. The provisions of the Rules of Court, Rules on Electronic Evidence, and other relevant rules and regulations under the Anti Wire-tapping Act and the Bank Secrecy Law shall apply in a supplementary character to this Circular.

**VII. EFFECTIVITY**

This Circular shall take effect immediately upon publication.



  
**MICHAEL G. AGUINALDO**  
Chairperson

  
**ROLAND C. PONDOC**  
Commissioner

*(Letterhead of the Audited Agency)*

**MANAGEMENT REPRESENTATION LETTER**

Date

**Cluster/Regional Director**  
Cluster/Regional Office  
Commission on Audit

**Subject: Submission of electronic document by [Name of Agency/  
Corporation/LGU/Project Being Audited]**

This representation letter is provided in connection with your audit of the financial statements of the [Agency/Corporation/LGU/Project] for the purpose of expressing opinions as to whether the financial statements are presented fairly, in all material respects, in accordance with International Public Sector Accounting Standards (IPSAS) and government accounting standards, and as to other terms required by the 1987 Constitution or other relevant laws.

**Specific Affirmations pertaining to Digitally-signed Electronic Documents  
Provided to the Commission on Audit**

We certify that the [Agency/Corporation/LGU/Project] is implementing and will continuously review and ensure a secured process such that the documents submitted to COA with digital signature shall bear the valid and authentic signature of its appropriate signatories.

We further certify that:

1. Appropriate security procedures were made to maintain the integrity, reliability, and authenticity of the information provided;
2. All the persons who have applied for Digital Certificates shall take full responsibility and accountability for all actions performed using their digital certificates;
3. We verified that all electronic documents submitted are either original or faithful electronic reproductions or duplicate copy of the paper-based documents; and
4. In case of digitized document, we certify that the original, as the source of the digitized document is authentic.

9

L

The above certifications are supported by the Confirmation Report of our Internal Audit Unit [or Compliance Unit or its equivalent] dated [Date], a copy of which is attached to this Representation Letter.

**Specific Affirmations pertaining to the use of Electronic Signature other than Digital Signature on Documents Provided to the Commission on Audit**

We certify that the [Agency/Corporation/LGU/Project] is implementing and will continuously review and ensure a secured process such that the documents submitted to COA with electronic signature shall bear the valid and authentic signature of its appropriate signatories.

We further certify that the system being employed for this purpose can reasonably ensure that:

1. Appropriate security procedures were made to maintain the integrity, reliability, and authenticity of the information provided;
2. The electronic signatures that appear on electronic documents belong to the persons to whom they correlate;
3. Every time an electronic signature is affixed, the intention is for authenticating or approving the electronic document to which it is related or to indicate consent to the transaction embodied therein;
4. The methods or processes utilized to affix or verify the electronic signature, operated every time without error or fault; and
5. The persons whose e-signatures were affixed have made a manifestation under oath to take responsibility and assume accountability that the documents bearing their e-signatures remained unchanged until they were submitted to the auditor.

The above certifications are supported by the Confirmation Report of our Internal Audit Unit [or Compliance Unit or its equivalent] dated [Date], a copy of which is attached to this Representation Letter.

**Admission of Estoppel on the Authenticity of Documents**

We attest and certify that any document bearing our electronic signature (including digital signature) submitted to the auditor is authentic and accurate, thus can be submitted to any court as required under a subpoena duces tecum or can be used as a legal document for other purposes.

Finally, we certify that, as supported by the Confirmation Report attached, we have taken appropriate measure to ensure that all and any electronic documents submitted to the auditor complies with definition of Original of Document in Section 4, Rule 30 of the 2019 Amendments to the 1989 Revised Rules on Evidence. The originals shall still be available for examination or inspection when needed.

9

We make this representation and request the auditor to accept electronic documents submitted by this [Agency/Corporation/LGU/Project] in addition or in combination with other paper documents.

Signed:

Signature over Printed Name  
Chief Accountant/Head of Finance Group

Signature over Printed Name  
Head of Agency/Authorized Representative

Date

Date

*Note:*

1. If the audited entity only uses digital signature on documents, the section for electronic signature should be deleted.
2. If the audited entity only uses electronic signature other than digital signature, the section for digital signature should be deleted.
3. If the audited entity uses a combination of electronic signatures including digital signature, both sections should be retained.





DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES  
KAGAWARAN NG KAPALIGIRAN AT LIKAS NA YAMAN



MEMORANDUM CIRCULAR  
No. 202\_-\_\_

SUBJECT: INTERNAL GUIDELINES ON THE USE OF ELECTRONIC DOCUMENTS AND DIGITAL SIGNATURES IN THE DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES (DENR)

In line with our commitment to efficient public service delivery and pursuant to Republic Act (RA) 8792<sup>1</sup>, RA 11032<sup>2</sup>, Government Procurement Policy Board (GPPB) Resolution No. 16-2019<sup>3</sup> and the Commission on Audit (COA) Circular No. 2021-006<sup>4</sup> dated 06 September 2021, the DENR adopts the following Guidelines on the Use of Electronic Documents and Digital Signatures in all official and internal documents, transactions, communication and processes in the DENR.

**SECTION 1. Basic Policy.** The State recognizes the vital role of information and communications technology (ICT) in nation-building. Its obligation is to facilitate the transfer and promotion of the adoption of technology for the national benefit.

**SECTION 2. Objectives**

- 2.1 To establish and implement controls and secure means of ensuring that the use of electronic documents and digital signatures within DENR meets requirements for validity, security, and authenticity.
- 2.2 To streamline official transactions within DENR through the use of electronic documents and digital signatures to enhance workflow efficiency and expedite decision-making processes.
- 2.3 To support environmental sustainability goals by minimizing paper usage and promoting eco-friendly practices through the adoption of electronic document workflows and digital signatures, contributing to the reduction of carbon footprint and resource consumption.

<sup>1</sup> Republic Act No. 8792 dated 14 June 2000, "Electronic Commerce Act of 2000"

<sup>2</sup> RA 11032 dated 28 May 2018, "Ease of Doing Business and Efficient Delivery of Government Service Delivery of 2018"

<sup>3</sup> Government Procurement Policy Board (GPPB) Resolution No. 16-2019 dated 17 July 2019, "Approval of the Use of Digital Signature in Procurement Related Documents"

<sup>4</sup> Commission on Audit (COA) Circular No. 2021-006 dated 06 September 2021, "Guidelines on the Use of Electronic Documents, Electronic Signatures and Digital Signatures in Government Transactions"

38 2.4 To align with broader government initiatives for digital transformation by  
39 tapping technology to modernize administrative practices, improve service  
40 delivery and contribute to the overall efficiency and effectiveness of DENR's  
41 operations in the digital age.  
42

43 **SECTION 3. Scope and Coverage.** This Circular shall apply in the event that  
44 the DENR officials and employees issue electronic documents in lieu of paper  
45 documents, where the signature of the authorized signatory is required. This  
46 Memorandum Circular does not intend to prohibit the office from submitting paper  
47 documents or a combination of paper and electronic documents.  
48

49 All DENR officials and personnel regardless of employment status in the DENR  
50 Central Office, Line and Staff Bureaus, Regional Offices, PENROs, CENROs,  
51 attached agencies, and locally funded and foreign-assisted projects, who are required  
52 to review and authorized to sign any official and/or internal documents pursuant to RA  
53 No. 11032, COA Circular No. 2021-006 or GPPB Resolution No. 16-2019 shall be  
54 governed by these guidelines.  
55

56 This also applies to electronic documents from private parties transacting with  
57 DENR offices.  
58

#### 59 **SECTION 4. Definition of Terms**

- 60
- 61 a. **Asymmetric of public cryptosystem<sup>5</sup>** - more commonly referred to as  
62 public key infrastructure, means a system capable of generation a secure  
63 key pair, consisting of a private key for creating digital signature, and a  
64 public key for verifying the digital signature.
- 65 b. **Certificate Authority (CA)<sup>6</sup>** - refers to a trusted entity that manages and  
66 issues security certificates and public keys that are used for secure  
67 communication in a public network or the internet. The DICT is the  
68 authorized Certificate Authority in the government.
- 69 c. **Certificate Revocation List<sup>7</sup>** - refers to a list of digital certificates that  
70 would have been compromised, revoked, or are expired.
- 71 d. **Confirmation Report - (to be provided by COA)**
- 72 e. **Digital Certificate<sup>8</sup>** - is a .p12 file issued by the Department of Information,  
73 Communication and Technology - Philippine National Public Key  
74 Infrastructure (DICT-PNPKI) or other CA containing the user's personal  
75 information just like an ordinary ID, only in this case, it is digital. It is used to  
76 encrypt, authenticate or digitally sign an email and document.
- 77 f. **Digital Signature<sup>9</sup>** - refers to a secure type of electronic signature  
78 consisting of a transformation of an electronic document or an electronic

<sup>5</sup> COA Circular No. 2021-006 dated 06 September 2021, "Guidelines on the Use of Electronic Documents, Electronic Signatures and Digital Signatures in Government Transactions"

<sup>6</sup> COA Circular No. 2021-006 dated 06 September 2021, "Guidelines on the Use of Electronic Documents, Electronic Signatures and Digital Signatures in Government Transactions"

<sup>7</sup> DICT Order No. 031 dated 01 April 2024, "Guidelines on the Use of PNPKI Digital Signatures in the DICT"

<sup>8</sup> DICT Order No. 031 dated 01 April 2024, "Guidelines on the Use of PNPKI Digital Signatures in the DICT"

<sup>9</sup> Rule 2 § 1 (e), "Rules on Electronic Evidence", A.M. No. 01-7-01-SC, 17 July 2001.

79 data message using an asymmetric or public cryptosystem such that a  
80 person having the initial untransformed electronic document and the  
81 signer's public key can accurately determine:

- 82 i. Whether the transformation was created using the private key that  
83 corresponds to the signer's public key; and
- 84 ii. Whether the initial electronic document had been altered after the  
85 transformation was made.

86 **g. Electronic Document<sup>10</sup>** - refers to information or the representation of  
87 information, data, figures, symbols or other modes of written expression,  
88 described or however represented, by which a right is established or an  
89 obligation extinguished, or by which a fact may be proved and affirmed,  
90 which is received, recorded, transmitted, stored, processed, retrieved or  
91 produced electronically.

92 **h. Key Pair<sup>11</sup>** - refers to the two mathematically related keys, the public and  
93 private keys. Whatever is encrypted with a Public Key may only be  
94 decrypted by its corresponding Private Key and vice versa. Public and  
95 private keys are paired for secure communication, such as email.

96 **i. Management Representation Letter - (to be provided by COA)**

97 **j. Private Key<sup>12</sup>** - is also a bit of code that is paired with a public key to set  
98 off algorithms for text encryption and decryption. It is created as part of  
99 public key cryptography during asymmetric-key encryption and used to  
100 decrypt and transform a message to a readable format. A private key is also  
101 known as a secret key.

102 **k. Public Key<sup>13</sup>** - is also a bit of code used to encrypt data. The is provided  
103 by the CA and is made available to everyone through a directory or email.

104 **l. Public Key Infrastructure (PKI)<sup>14</sup>** - is an infrastructure that secures  
105 communications among individuals and government entities. This way, the  
106 government's delivery of services to citizens and businesses becomes  
107 safer, faster and more efficient.

108 **m. Wet Signature<sup>15</sup>** - refers to a physical signature made by hand with ink on  
109 paper. It is often used in legal and formal documents to signify acceptance,  
110 authorization, or verification. The concept of a wet signature is rooted in  
111 traditional practices of signing documents by hand, dating back centuries

112  
113  
114  
115  
116  
117  
118  

---

<sup>10</sup> Section 5 (f), RA No. 8792 dated 14 June 2000, "Electronic Commerce Act of 2000"

<sup>11</sup> DICT Order No. 031 dated 01 April 2024, "Guidelines on the Use of PNPKI Digital Signatures in the DICT"

<sup>12</sup> DICT Order No. 031 dated 01 April 2024, "Guidelines on the Use of PNPKI Digital Signatures in the DICT"

<sup>13</sup> DICT Order No. 031 dated 01 April 2024, "Guidelines on the Use of PNPKI Digital Signatures in the DICT"

<sup>14</sup> DICT Order No. 031 dated 01 April 2024, "Guidelines on the Use of PNPKI Digital Signatures in the DICT"

<sup>15</sup> ChatGPT

119 **SECTION 5. Guidelines**

120 **A. General Principles and Guidelines**

- 121
- 122 1. DENR digital signature shall be an accepted alternative and be equivalent to
- 123 the signature of a person on a paper/physical document.
- 124
- 125 2. DENR shall ensure data protection and implement cybersecurity measures in
- 126 accordance with the following laws, but not limited to:
- 127 a. Data Privacy Act of 2012 or RA No. 10173 dated 12 August 2012
- 128 b. Cybercrime Prevention Act of 2012 or RA No. 10175 dated 12
- 129 September 2012
- 130 c. Executive Order (EO) No. 2<sup>16</sup> dated 23 July 2016
- 131 d. applicable DICT issuances
- 132
- 133 3. To ensure secure transactions, private parties interacting with DENR may
- 134 utilize alternative digital signing methods, subject to approval and security
- 135 controls established by the concerned DENR office.
- 136
- 137 4. The Internal Audit Service (or its equivalent unit in other DENR offices) shall
- 138 provide a Confirmation Report to the Accounting Division (or its equivalent
- 139 unit in other DENR offices). This shall be attached to the Management
- 140 Representation Letter (ANNEX A) for submission to their respective resident
- 141 auditors.
- 142
- 143
- 144
- 145
- 146
- 147
- 148
- 149
- 150
- 151
- 152
- 153
- 154
- 155
- 156
- 157
- 158
- 159
- 160
- 161
- 162
- 163
- 164

---

<sup>16</sup> Executive Order No. 2 dated 23 July 2016, "Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor"



165  
166  
167

5. The following are the authorized signatories for the Management Representation Letter:

	Central Office	Regional Offices	Bureaus	Attached Agencies
Signed	<ol style="list-style-type: none"> <li>1. Director, Financial and Management Service;</li> <li>2. Director, Knowledge and Information Systems Service (KISS); and</li> <li>3. Supervising Undersecretary or Authorized Representative</li> </ol>	<ol style="list-style-type: none"> <li>1. Chief, Finance Division</li> <li>2. Chief Supervising the ICT Unit</li> <li>3. Assistant Regional Director for Management Services or Authorized Representative</li> </ol>	<ol style="list-style-type: none"> <li>I. Staff Bureaus               <ol style="list-style-type: none"> <li>1. Chief Supervising the Accounting Unit</li> <li>2. Chief Supervising the ICT Unit</li> <li>3. Bureau Director or Authorized Representative</li> </ol> </li> <li>II. Line Bureaus               <ol style="list-style-type: none"> <li>A. MGB                   <ol style="list-style-type: none"> <li>A.1 MGB - CO                       <ol style="list-style-type: none"> <li>1. Chief Supervising the Accounting Unit</li> <li>2. Chief Supervising the ICT Unit</li> <li>3. Bureau Director or Authorized Representative</li> </ol> </li> <li>A.2 MGB RO                       <ol style="list-style-type: none"> <li>1. Chief Supervising the Finance Section</li> <li>2. Chief Supervising the ICT Unit</li> <li>3. Regional Director or Authorized Representative</li> </ol> </li> </ol> </li> <li>B. EMB                   <ol style="list-style-type: none"> <li>B.1 EMB - CO                       <ol style="list-style-type: none"> <li>1. Chief, AFMD</li> <li>2. Chief Supervising the ICT Unit</li> <li>3. Bureau Director or Authorized Representative</li> </ol> </li> <li>B.2 EMB - RO                       <ol style="list-style-type: none"> <li>1. Chief, FAD</li> <li>2. Chief Supervising the ICT Unit</li> <li>3. Regional Director or Authorized Representative</li> </ol> </li> </ol> </li> </ol> </li> </ol>	<ol style="list-style-type: none"> <li>1. Chief Supervising the Accounting Unit</li> <li>2. Chief Supervising the ICT Unit</li> <li>3. Head of Office or Authorized Representative</li> </ol>

DRAFT

168  
169  
170  
171  
172  
173  
174  
175

## **B. Specific Guidelines on the Use of Digital Signatures**

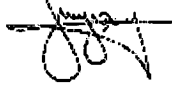
- 176 1. DENR officials and employees regardless of employment status who are  
177 required to review and authorized to sign official documents may use a  
178 digital signature. They shall apply for a digital certificate at the Philippine  
179 National Public Key Infrastructure (PNPKI) of the DICT and/or other  
180 Certificate Authorities through the assistance of the KISS or its equivalent  
181 unit in other DENR Offices.  
182  
183  
184
- 185 2. At a minimum, the implementation of digital signatures shall bear the  
186 following characteristics:  
187 a. Authentication - linking the signatory to the information;  
188 b. Integrity – assuring that the document has not been altered during  
189 transmission; and  
190 c. Non-repudiation – ensuring that the signer of the electronic document  
191 cannot at a later time deny having signed it.  
192
- 193 3. When using a digital certificate to sign an electronic document, the same  
194 should be valid, unexpired, and unrevoked at the time of signing. The  
195 digital certificate is valid for up to two years upon approval from DICT. The  
196 certificate owner shall have to apply for a new one before its expiration.  
197
- 198 4. Officials/employees with expiring digital certificates and about to retire in  
199 a year shall no longer renew their digital certificates.  
200
- 201 5. Resigning permanent employees with active digital certificates are  
202 required to submit a written request for revocation of their digital  
203 certificates to KISS (or its equivalent unit in other DENR offices) with a  
204 copy furnished to the Human Resource Development Service (or its  
205 equivalent unit in other DENR offices). The Supervisors of the  
206 resigning/transferring employees shall not sign the DENR Office  
207 Clearance (Item II Clearance from Work Accountabilities) without the  
208 revocation of the digital certification.  
209
- 210 6. Permanent employees with active digital certificates which will be  
211 transferred to other DENR offices shall retain their existing digital  
212 certificates. However, those transferring to attached agencies and other  
213 government agencies shall be governed by Section 5.B Specific  
214 Guidelines on Use of Digital Signatures, item no. 6 of this Memorandum  
215 Circular.  
216
- 217 7. Supervisors of resigning/resigned Contract of Service (COS)/Job Order  
218 (JO) personnel with active digital certificates shall be required to submit a  
219 written request for revocation of their staff's digital certificates to KISS (or  
220 its equivalent unit in other DENR offices) with a copy furnished to the  
221 Human Resource Development Service (or its equivalent unit in other  
222 DENR offices).  
223  
224

225 8. The following details in a human-readable form, shall accompany the  
226 digital signatures:

227 9.1 For Digital Full Signature:

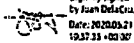
- 228 a. Full name of the signatory; and
- 229 b. Image of the full signatory's handwritten signature;

230  
231 Example of a properly formatted digital signature

232 Digitally signed  
233 by Juan DelaCruz  
234  Date: 2020.05.21  
235 19:37:33 +08'00'

236  
237 8.2 Digital Initial Signature Format:

- 238 a. For officials/employees who are required to review official  
239 documents before the signing, they may use smaller images as  
240 their initials as shown below:

241  
242   
243 Digitally signed  
244 by Juan DelaCruz  
245 Date: 2020.05.21  
246 19:37:33 +08'00'

244 However, other formats shall be acceptable for digital full signature and  
245 initial signature as long as they clearly display the full name of the  
246 signatory and an image of the signatory's handwritten signature.

247  
248   
249 Sep 01 2020 08:49:51  
250 ATTY. EDUARDO V. BRINGAS  
251 Deputy Director General

### 252 C. Specific Guidelines on the Use of Electronic Documents

- 253 1. Using digital signatures in electronic documents shall follow the guidelines  
254 stated in this Memorandum Circular and shall mean sufficient compliance  
255 with the requirement of submission of duly signed documents as any other  
256 duly signed paper document used in DENR transactions.
- 257 2. Electronic documents must be digitally signed in a secured computer and  
258 network system that complies with the prescribed cybersecurity protocols  
259 as mandated by relevant laws, rules and regulations.
- 260 3. The affixed digital signature to the electronic document shall be  
261 protected/locked to ensure the document will not be altered.
- 262 4. The digitally signed documents shall be stored in a secured file format,  
263 such as Portable Document Format (PDF). Any other compatible formats  
264 may also be used, provided they allow secure implementation of digital  
265 signatures.
- 266 5. The digitally signed documents shall be considered the final version once  
267 they are released or transmitted to their intended recipients. The digitally  
268 signed documents shall be passed through official domain emails  
269 (e.g.name@denr.gov.ph) to have a trace.

- 275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287
6. Reproduction of digitally signed documents are considered duplicates or secondary copies. A notation (footer) or disclosure "*This original of this document is in digital format*" shall be indicated on the duplicate copies.
  7. In cases where mixed signing occurs in a single document, the signer is responsible for ensuring the authenticity of the document before he/she signs it in digital or wet form. Mixed signing occurs when a document is either:
    - a. Initially wet signed which was thereafter scanned/photographed and later digitally signed, or
    - b. Digitally signed which was thereafter printed out and later wet signed.

## **SECTION 6. DUTIES AND RESPONSIBILITIES**

### **A. KISS - DENR Central Office**

- 288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322
1. Assist all officials/employees in the DENR Central Office, Line and Staff Bureaus, Regional Offices, PENROs, CENROs and Attached Agencies on the application and validation of digital signature certificates at the DICT under PNPKI, and monitor the status of digital signature applicants and users.
  2. Develop a system and provide secure storage for electronically signed documents including supporting/attaching documents.
  3. Conduct training or orientation to disseminate information on the use of electronic documents and digital signatures, including a security awareness program, in coordination with HRDS and DICT. This shall cover all offices in the Central Office, Bureaus, Regional Offices, PENROs and CENROs and Attached Agencies.
  4. Assist officials/employees in the downloading and installation of the digital signatures.
  5. Provide responses/clarifications on queries and concerns related to the application, download, installation, and use of digital certificates.
  6. Initiate the necessary procedures to request the revocation of compromised certificates to DICT.
  7. Submit a report to the Commission on Audit (COA) Resident Auditor in case of revocation or expiration (without renewal) of the digital certificates. Certificate Revocation List must be kept updated, which contains the list of digital certificates that would have been compromised or expired.
  8. Provide other technical assistance as may be directed.

323 **B. ICT Units in the DENR Regional Offices, PENROs and CENROs, Bureaus**  
324 **and Attached Agencies**

- 325
- 326 1. Assist all officials/employees on the application and validation of digital  
327 signature certificates in coordination with KISS.
- 328
- 329 2. Assist officials/employees in their respective offices in the downloading  
330 and installation of the digital signatures.
- 331
- 332 3. Provide responses/clarifications to their respective offices on queries and  
333 concerns related to the application, download, installation, and use of  
334 digital certificates.
- 335
- 336 4. Monitor the status of digital signature owners in their respective offices  
337 and submit reports to KISS.
- 338
- 339 5. Initiate the necessary procedures to request the revocation of  
340 compromised certificates to DICT.
- 341
- 342 6. Submit a report to the Commission on Audit (COA) Resident Auditor in  
343 case of revocation or expiration (without renewal) of the digital certificates  
344 and furnish a copy to KISS. Certificate Revocation List must be kept  
345 updated, which contains the list of digital certificates that would have been  
346 compromised or expired.
- 347
- 348 7. Provide other technical assistance as may be directed.
- 349

350 **C. Digital Certificate/Signature Owner**

- 351
- 352 1. All officials and employees who applied for Digital Certificates shall take  
353 full responsibility and accountability for all actions executed using the  
354 digital certificate.
- 355
- 356 2. Digital signatures are electronic files that can be stored in storage devices  
357 such as computers, flash drives or any cloud storage, hence, the owner  
358 shall take full responsibility for its usage and storage to ensure the integrity  
359 and non-repudiation of the signatures.
- 360
- 361 3. All digital certificate owners shall immediately notify the KISS (or its  
362 equivalent unit in other DENR offices) in the following instances:
- 363 a. If the digital certificate is compromised (i.e., forgotten password,  
364 lost certificate, etc.);
- 365 b. In case of a breach or security compromise in the device that stores  
366 the digital certificate; or
- 367 c. If the digital certificate owner is leaving as DENR personnel (either  
368 from plantilla, contractual, or job order) due to resignation,  
369 retirement, or service termination.
- 370
- 371
- 372

373 **D. Internal Audit Service/Division/Section/Unit**

- 374
- 375 1. Provide Confirmation Report to Accounting Division/Section/Unit as
- 376 attachment to the Management Representation Letter prior its submission
- 377 to COA.
- 378

379 **E. Accounting Division/Section/Unit**

- 380
- 381 1. Prepare and submit a Management Representation Letter in coordination
- 382 with KISS (or its equivalent in other DENR offices). The submission to
- 383 COA shall include a Confirmation Report and the approved Internal
- 384 Guidelines on the Use of Electronic Documents and Digital Signatures
- 385 (TIMELINE of submission for consultation with COA).
- 386

387

388 **SECTION 7. Limitations**

389 Digital signatures shall not apply on the following:

- 390 1. Contracts and agreements and other related documents that require
- 391 notarization.
- 392 2. Other DENR-issued documents/forms that have other security
- 393 features/controls (i.e., ?????????) unless allowed by the Department.
- 394

395 **SECTION 8. Administrative Sanctions.** Any violation or non-compliance of

396 one or more provisions of this Memorandum Circular shall be dealt with by the

397 competent national authorities concerned in accordance with relevant applicable laws,

398 rules and regulations.

399

400 **SECTION 9. Separability Clause.** If any provision of this Circular shall be held

401 invalid or unconstitutional, the other portions or provisions hereof which are not

402 affected shall continue in full force and effect.

403

404 **SECTION 10. Repealing Clause.** All Circulars and other similar issuances

405 inconsistent herewith are hereby revoked, amended, or modified accordingly.

406

407 **SECTION 11. Effectivity.** This Memorandum Circular shall take effect

408 immediately.

409

410

411

412 **MARIA ANTONIA YULO LOYZAGA**

413 Secretary

414  
415 **(Official Letterhead of the Audited Agency)**  
416

417  
418 **MANAGEMENT REPRESENTATION LETTER**  
419

420 Date

421  
422  
423 **Cluster/Regional Director**

424 Cluster/Regional Office

425 Commission on Audit  
426

427 **Subject: Submission of electronic document by [Office Being Audited]**  
428

429  
430 This representation letter is provided in connection with your audit of the financial  
431 statements of the [Office] for the purpose of expressing opinions as to whether the  
432 financial statements are presented fairly, in all material respects, in accordance with  
433 International Public Sector Accounting Standards (IPSAS) and government  
434 accounting standards, and as to other terms required by the 1987 Constitution or other  
435 relevant laws.  
436

437 **Specific Affirmations pertaining to Digitally-signed Electronic Documents**  
438 **Provided to the Commission on Audit**  
439

440  
441 We certify that the [Office] is implementing and will continuously review and  
442 ensure a secured process such that the documents submitted to COA with  
443 digital signature shall bear the valid and authentic signature of its appropriate  
444 signatories.  
445

446 We further certify that:

- 447
- 448 1. Appropriate security procedures were made to maintain the integrity,  
449 reliability, and authenticity of the information provided;
  - 450 2. All the persons who have applied for Digital Certificates shall take full  
451 responsibility and accountability for all actions performed using their  
452 digital certificates;
  - 453 3. We verified that all electronic documents submitted are either original  
454 or faithful electronic reproductions or duplicate copy of the paper-based  
455 documents; and
  - 456 4. In case of digitized document, we certify that the original, as the source  
of the digitized document is authentic.

457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482

The above certifications are supported by the Confirmation Report of our Internal Audit Unit [or Compliance Unit or its equivalent] dated Date], a copy of which is attached to this Representation Letter.

**Admission of Estoppel on the Authenticity of Documents**

We attest and certify that any document bearing our digital signature submitted to the auditor is authentic and accurate, thus can be submitted to any court as required under subpoena duces tecum or can be used as a legal document for other purposes.

Finally, we certify that, as supported by the Confirmation Report attached, we have taken appropriate measures to ensure that all and any electronic documents submitted to the auditor comply with the definition of Original of Document in Section 4, Rule 30 of the 2019 Amendments to the 1989 Revised Rules on Evidence. The originals shall still be available for examination or inspection when needed.

We make this representation and request the auditor to accept electronic documents submitted by this [Office] in addition or in combination with other paper documents.

***"SAMPLE AUTHORIZED SIGNATORIES IN DENR CENTRAL OFFICE"***

Signed:

(Director, FMS)

(Director, KISS)

Date:

Date:

(Undersecretary for FISCC)

Date:

483  
484