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[1] 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.

[1] 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[2] and the Cybercrime Prevention Act of 2012[3] 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.

---

[2] 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.
[3] 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.[4]

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-PNPKI 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.[5]

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.[6]

---

[4] Rules on Electronic Evidence, A.M. No. 01-7-01-SC, July 17, 2001, Rule 2, Section 1(a).
[5] Rules on Electronic Evidence, Rule 2, Section 1(e).
[6] 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.[7] 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.[8]

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.

---

[7] Rules on Electronic Evidence, Rule 2, Section 1(j).

[8] Dave Venance, What is an e-Signature? Part I, *available at* 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.

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.[9]

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

[9] Executive Order No. 810, June 15, 2009, Section 3(d).

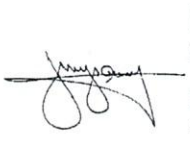
signed e-mails, it is recommended that a government domain email be used (e.g. name@agency.gov.ph)

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:



    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. SUPPLETORY 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 suppletory character to this Circular.

VII. EFFECTIVITY

This Circular shall take effect immediately upon publication.

MICHAEL G. AGUINALDO
Chairperson

COMMISSION ON AUDIT
OFFICE OF THE COMMISSION SECRETARIAT

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.

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.

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	**Signature over Printed Name**
Chief Accountant/Head of Finance Group	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.