

MALACAÑANG
Manila

BY THE PRESIDENT OF THE PHILIPPINES

EXECUTIVE ORDER NO. 810

INSTITUTIONALIZING THE CERTIFICATION SCHEME FOR DIGITAL SIGNATURES AND DIRECTING THE APPLICATION OF DIGITAL SIGNATURES IN E-GOVERNMENT SERVICES

WHEREAS, lack of security has been perceived as the main barrier for growth of electronic commerce and wide use of e-government services in the country;

WHEREAS, there is a need to provide a secure infrastructure for the exchange of data or information in information and communications technology (ICT) systems;

WHEREAS, there is a need to ensure the protection of parties involved in electronic transactions with regard to privacy, confidentiality and content control;

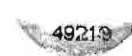
WHEREAS, an electronic signature represents the identity of the person attached to or associated with an electronic data message or electronic document, employing any methodology or procedure to authenticate or approve the electronic data message or electronic document;

WHEREAS, Section 8 of Republic Act No. 8792 or the Electronic Commerce Act of 2000 provides for the legal recognition of electronic signatures and imposes strict requirements before an electronic signature qualifies as a handwritten signature;

WHEREAS, by imposing such strict requirements to prove the authenticity, integrity and reliability of electronic signatures, the Electronic Commerce Act validates only electronic signatures, which include, but are not limited to, digital signatures, which are generated through technology that complies with all the requirements enumerated in the Act;

WHEREAS, the Rules on Electronic Evidence issued by the Supreme Court in 2001 in accordance with the provisions of the Electronic Commerce Act, defines digital signature as "an 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";

WHEREAS, there is a need to institutionalize a certification scheme for digital signatures in the country and designate specific agencies in government which will provide the necessary services to implement the scheme;



NOW, THEREFORE, I, GLORIA MACAPAGAL-ARROYO, President of the Republic of the Philippines, by virtue of the power vested upon me by law, do hereby order:

Section 1. *Adopting a Framework for National Certification Scheme for Digital Signatures.* A National Certification Scheme for Digital Signatures in the Philippines, as it appears in Annex A, is hereby adopted.

Section 2. *Guidelines to Implement the National Certification Scheme for Digital Signatures in the Philippines.* The Department of Trade and Industry (DTI) shall, by virtue of its mandate under the Electronic Commerce Act, issue the necessary guidelines to implement the National Certification Scheme for Digital Signatures in the Philippines.

Section 3. *Designation of Government Agencies and Functions.* The following agencies are hereby designated to perform the necessary services under the certification scheme:

- a) **Root Certification Authority (CA)**. The National Computer Center (NCC) under the Commission on Information and Communications Technology (CICT) is hereby designated to operate the Root CA. As such, it shall perform the following functions:
1. operate the Root CA system;
 2. issue and manage certificates to accredited government and private CAs;
 3. develop and prescribe technical standards for digital signatures in collaboration with the Bureau of Product Standards of the Department of Trade and Industry (DTI);
 4. develop certification technology;
 5. ensure interoperability of digital certification technology;
 6. provide technical expertise in the conduct of assessment of CAs when necessary;
 7. support international cooperation on certification services including mutual recognition and cross-certification;
 8. resolve disputes involving the issuance and use of digital certificates between concerned parties.
- b) **Government Certification Authority (CA)**. The NCC is likewise designated to operate the Government CA. As such, it shall perform the following functions:
1. issue certificates for all government transactions to government employees/entities and specific purpose certificates to private individuals/entities;
 2. publish certificates and Certificate Revocation List (CRL);
 3. handle revocation requests from the owners of the certificates it has issued.
- c) **Registration Authority (RA)**. Government agencies and instrumentalities providing e-government services to its clients shall perform the following functions as RA:
1. identify the user and register the user information;
 2. transmit certificate request to government CA;
 3. validate certificates from the CA directory server and CRL;
 4. request revocation of certificates.



- d) **Accreditation and Assessment Body.** The Department of Trade and Industry (DTI), through its Philippine Accreditation Office (PAO), is hereby designated as the accreditation and assessment body for CAs pursuant to its mandate and in accordance with the provisions of the E-Commerce Act. As such, DTI shall perform the following functions:
1. Issue the necessary criteria and guidelines for accreditation of CAs to ensure security and interoperability of systems and certificates, as well as compliance with the prescribed standards for digital signatures;
 2. Accredite CAs, whether government or private, according to the prescribed criteria and guidelines for accreditation;
 3. Conduct regular assessment of CAs to ensure compliance to existing criteria, guidelines and standards;
 4. Revoke or suspend the license of a CA for failure to comply with prescribed guidelines and standards;
 5. Create an Advisory Committee which shall provide direction and advice on the formulation of policies pertaining to the scheme for accreditation and assessment of CAs;
 6. Create other committees to perform such other functions as may be determined indispensable and necessary to efficiently, effectively and expediently pursue the duties defined under this sub-section.

Section 4. Application of Digital Signatures in E-Government Services. All government agencies and instrumentalities providing electronic services to its clients shall require the use of digital signatures in their respective e-government services to ensure confidentiality, authenticity, integrity and non-repudiation of electronic transactions in government. Such projects shall be included in the Information Systems Strategic Plan (ISSP) which government agencies are required to submit to NCC-CICT for approval and endorsement to the Department of Budget and Management (DBM) .

The NCC-CICT shall plan, direct and monitor the implementation of this provision in government. Accordingly, it shall assist concerned agencies designated as RA to ensure the smooth implementation of the system.

Within three (3) months from the issuance of this Order, NCC-CICT shall submit to the Office of the President the implementation plan including timetable and required resources to implement this Order. The plan shall identify priority government agencies and instrumentalities and the respective e-government services that will be required to comply within two (2) years from the issuance of this Order. Other government agencies and instrumentalities shall be given three (3) years to comply with this Order.

Section 5. Funding and Manpower. To fast-track the implementation of this Order, CICT is hereby directed to prioritize projects of government agencies which are applying for funding under the E-government Fund for projects that will immediately apply the use of digital signatures in their respective e-government services. Such



PGMA Hologram # 49221



projects remain subject to the requirements of the E-government Fund and must be identified in the agencies' NCC-approved ISSP.

All government agencies and instrumentalities concerned shall submit its manpower and budgetary requirements to the Department of Budget and Management (DBM) to implement this Order. The DBM is hereby directed to ensure that resources will be appropriated in the regular budget of government agencies to implement this Order in consultation with DTI and CICT.

Section 6. Application of Digital Signatures in ICT Systems in the Private Sector. In line with its mandate to promote electronic commerce in the country, the DTI shall promote the application of digital signatures in ICT systems in the private sector to ensure confidentiality, authenticity, integrity and non-repudiation of electronic transactions with the private sector,

Government agencies or entities exercising supervisory and regulatory functions over private services are hereby directed to study and identify critical services that use electronic systems which require high levels of security for using and storing personal information and transactions, with the view of strictly requiring the use of digital signatures in such services.

Section 7. Fees. NCC, as Root CA and Government CA, is hereby authorized to charge fees for the issuance of digital certificates guided by the universal concept of user charges, which is to recover at least the full cost of services rendered. Similarly, government agencies and instrumentalities performing the functions of RA are authorized to charge fees for services rendered. In exceptional cases, however, government RAs may assume the cost of the digital certificates issued to subscribers subject to its contractual arrangement with the Government CA. The imposition of new fees or increases thereafter shall be subject to the provision of Memorandum Circular No. 137, Series of 2007, and National Economic and Development Authority (NEDA) Circular No. 01-2007.

The costs of digital certificates issued directly by private Accredited CAs (ACAs) or through their respective RAs shall be market-determined, just and reasonable. Private RAs have the option to assume the costs of the certificates issued to subscribers depending on its contractual arrangements with the ACA.

Section 8. Dispute Resolution. Cases arising from (1) the accreditation of CAs; (2) the use and issuance of digital certificates; (3) issues necessarily included therein; or (4) issues which include the same, shall be heard and resolved by the respective agencies designated to perform the necessary services in accordance with the rules and regulations to be formulated for such purpose.

Section 9. Transitory Provision. During the initial transitory period after the issuance of the Rules and Regulations to implement this Order, there shall be an interim personnel complement to manage and operate the Root CA and Government CA and perform the functions of the respective RAs. Such personnel can either be on detail, reassignment or secondment subject to existing rules of the Civil Service Commission on personnel movements.



PGMA Hologram # 49222

DTI and CICT shall determine and recommend to DBM the most appropriate mode of complementing the manpower requirements for the implementation of this Order.

In the interim, or until such time that a private ACA becomes operational, NCC shall assume the role of private ACA.

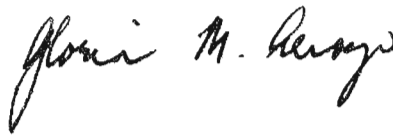
Section 10. Repealing Clause. All issuances, orders, rules and regulations, or parts thereof, which are inconsistent with the provisions of this Executive Order, are hereby repealed, amended or modified accordingly.

Section 11. Effectivity. This Order shall take effect immediately.

Done in the City of Manila this 15th day of June , in the year of Our Lord, Two Thousand and Nine.

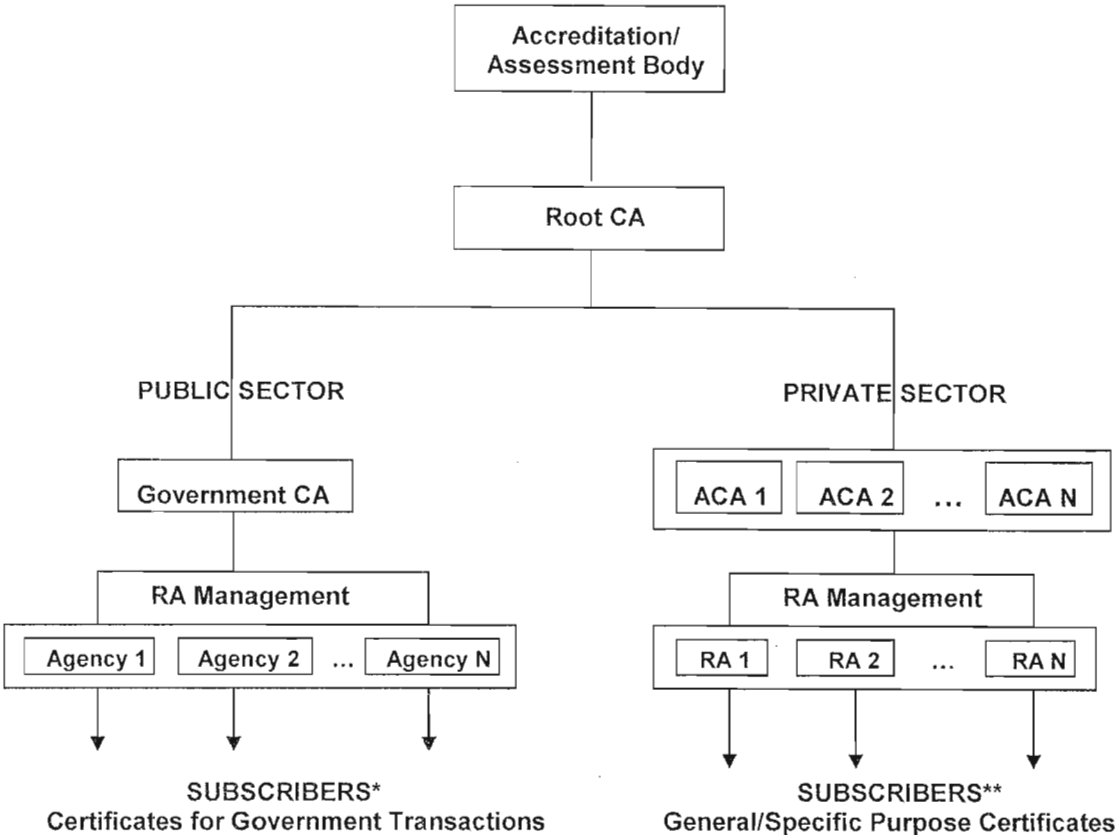
By authority of the President:


EDUARDO R. ERMITA
Executive Secretary





CERTIFICATION SCHEME FOR DIGITAL SIGNATURES



** Government employees/entities – certificates for all government transactions
Non-government individuals/entities – certificates specific to a government transaction
(specific purpose certificate)*

***Private individuals/entities and government employees*



DEFINITION OF TERMS:

Asymmetric or public cryptosystem – 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.

Accreditation and Assessment Body – refers to the body that accredits the CAs and conducts regular assessment of such CAs to ensure compliance to prescribed criteria, guidelines and standards.

Certificate – an electronic document issued to support a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair. Certificates issued may be for general use or for specific use only.

Certification Authority (CA) – issues digitally-signed public key certificates and attests that the public key embedded in the certificate belongs to the particular subscriber as stated in the certificate. A CA may be involved in a number of administrative tasks such as end-user registration, although these tasks are often delegated to the Registration Authority (RA). The CA may either be a government body or private entity.

Digital Signature – refers to an 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 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.

Electronic key – refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable only with a matching electronic key.

General Purpose Certificate – a certificate which can be used for all government and private transactions.

Registration Authority (RA) – refers to a third-party used by the CA to perform administrative tasks such as end-user registration. The RA may either be a government agency or private entity performing frontline services.

Root CA – issues and manages certificates to government and private CAs.

Specific Purpose Certificate – a certificate which can only be used for a specific transaction.

Subscriber – an individual or entity applying for and using digital certificates issued by the CA.



THE SCHEME:

The DTI, which is the Accreditation/Assessment Body under this scheme, shall issue the implementing guidelines and the criteria for the accreditation of the Root CA (NCC), the Government CA (NCC), and the private CA. The role of the Root CA is critical to ensure the interoperability of systems among accredited CAs and cross-recognition of certificates within and outside the country.

The Government CA will issue certificates to government employees and entities which can be used for all government transactions. The Government CA can also issue specific purpose certificates for a specific government transaction to private individuals and entities (e.g. private individual and corporate taxpayers) if they do not have a general purpose certificate issued by a private ACA. In both cases, the Government CA will issue the certificates through a government agency which shall function as RA.

Government employees have to apply for general or specific purpose certificates from a private ACA for personal transactions with private entities.

General purpose certificates issued by a private ACA to private individuals and entities can also be used for transactions with government. The private ACA may issue the certificates directly to the subscriber or through a private entity which shall function as RA.

