[EXECUTIVE ORDER NO. 810, June 15, 2009]

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, SEC. 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.

SEC. 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.

SEC. 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