[DTI DEPARTMENT ADMINISTRATIVE ORDER NO. 10-09, September 29, 2010]

PRESCRIBING RULES GOVERNING THE ACCREDITATION OF CERTIFICATION AUTHORITIES FOR DIGITAL SIGNATURES

Pursuant to the provisions of Republic Act No. 8792 otherwise known as the 'Electronic Commerce Act of 2000,' its lmplementing Rules and Regulations and the provisions of Executive Order No. 810 issued on 15 June 2009 and entitled, 'lnstitutionalizing the Certification Scheme for Digital Signatures and Directing the Application of Digital Signatures in E-Government Services," this Department Administrative Order is hereby prescribed for the compliance, information, and guidance of all concerned:

1. Scope

This Department Administrative Order prescribes the rules governing the Accreditation Scheme for Certification Authorities for Digital Signatures.

2. Definitions

The following definitions shall apply under this Order unless the context otherwise requires:

2.1 "Accreditation" - third-party attestation related to a Certification Authority conveying formal demonstration of its competence to carry out specific tasks.

2.2 "Accreditation and Assessment Body" - refers to the body that accredits the Certification Authorities (CAs) and conducts regular assessment of such CAs to ensure compliance to prescribed criteria, guidelines and standards; refers to the Philippine Accreditation Office (PAO).

2.3 "Accreditation Symbol" - symbol issued by an accreditation body to be used by accredited Certification Authorities to indicate their accredited status.

2.4 "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.

2.5 "Accreditation Certificate - the certificate granted under this Order.

2.6 "Certlficate" - 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 maybe for general use or for specific use only.

2.6.1. "General Certificate" - a certificate which can be used for all government and private transactions.

2.6.2. “Specific Purpose Certificate” - a certificate which can only be used for a specific purpose.

2.7 “Certificate Revocation List (CRL)” - a time-stamped list that identifies/contains revoked or invalid certificates. The CRL is signed by a Certification Authority and is published periodically in a public repository.

2.8 “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 maybe 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.

2.9 “Certification Practice Statement (CPS)”- a statement of the practices, which a CA employs in issuing and managing certificates, and addressing its general business liability and services availability.

2.10. “Compromise” - a case where the private key and related security information have been or may be stolen, or leaked, or where secrecy has been or maybe lost by a third party’s decryption.

2.11 “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 signers public key ; and (ii) whether the initial digital document had been altered after the transformation was made.

2.12. “DTI” refers to the Department of Trade and Industry.

2.13. “PAO” refers to the Philippine Accreditation Ofiice.

2.14. “Serious Misconduct”- any failure to comply with the requirements of the Electronic Commerce Act or this Order or its Certification Practice Statement and any act or omission relating to the conduct of business of a CA, which is or likely to be prejudicial to public interest.

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

2.16”Subscriber identity verification method” - the method used to verify and authenticate the identity of a subscriber.

2.17 “Substantial share holder - in relation to an a applicant, which is a company, means a person who owns or controls the voting rights to 10percent or more of the shares of the corporation.

2.18 “Trusted person” means any person who has —

Direct responsibilities for the day-to-day operations, security, and performance of those business activities that are regulated under this Order in respect of a CA.

Duties directly involving the issuance, renewal, suspension, revocation of certificates (including the identificationof any person requesting a certificate from an accredited CA), creation of private keys, or administration of a CA's computing facilities,

2.19. "This Order" refers to this Department Administrative Order.

3. Responsibilities for Accreditation

3.1. The DTl, through the PAO, shall operate the accreditation scheme for CAs for digital signatures. The operation of the scheme shall be under the direction of the PAO Council, which will be responsible for setting accreditation policies.

3.2. Responsibilities of PAO

3.2.1 In consultation with stakeholders, establish/update criteria for accreditation of CAs for digital signatures.

3.2.2 Receive and process a application for accreditation.

3.2.3 Organize teams to undertake assessment of applicants for accreditation.

3.2.4 Grant accreditation to applicant CAs found to comply with the established accreditation criteria.

3.2.5 Maintain and publish registry of duly accredited CAs.

3.2.6 Act on any verified complaints relating to accreditation of CAs.

3.2.7 Suspend or revoke accreditation of CAs found not consistently complying with the terms and conditions of accreditation.

3.3. Advisory Committee

3.3.1 The Advisory Committee shall be formed where stakeholders of the scheme will have the opportunity to give their inputs of the development of accreditation policies.

3.3.2 The Advisory Committee shall provide advice to the PAO Council on the formulation of policies pertaining to the operation of the PAO accreditation scheme for CAs for digital signatures.

3.3.3 Composition of the Advisory Committee:

3.3.3.1. One (1) representative from the Bangko Sentral ng Pilipinas;
3.3.3.2. One(1)representative from the National Computer Center;
3.3.3.3. One (1) representative from an Information and Communications Technology (lCT) Association;
3.3.3.4. One(1) representative from the National Telecommunications Commission:
3.3.3.5. One (1) Representative from Information Security Professionals Association(s)or its corresponding national chapter;

3.3.3.6. One (1) representative from a private CA; and
3.3.3.7. Other members, which maybe invited as deemed necessary.

3.4 Accreditation Evaluation Panel (AEP)

3.4.1 The AEP shall be composed of at least three (3) members drawn from the Advisory Committee or pool of PAO technical experts/subcontractors and to be knowledgeable on the applicable accreditation criteria for CAs.

3.4.2 The AEP evaluates final assessment reports, prepares and submits to the head of PAO its recommendation, which could either be a confirmation or reversal of the recomendations made by the assessment team.

4. Conditions for Accrecditation

4.1. Operational Criteria

4.1.1. The CA applying for accreditation must be duly registered with the Securities and Exchange Commission if a corporation or partnership; or with the Department of Trade and Industry, if it is a single proprietorship. Foreign CAs interested to set up their businesses in the Philippines must comply with applicable Philippine laws, rules and regulations and locate and operate their business within the country.

4.1.2 An applicant CA shall demonstrate through assessment of its offices and the observation of its certificate management/issuance process, that it satisfies PAO accreditation criteria.

4.1.3 The applicant CA shall have issued at least one(1) certificate to an entity.

4.1.4 The applicant CA shall agree to continuously comply with the terms and conditions of accreditation.

4.1.5 The applicant CA shall have a Certification Practice Statement (CPS) as referred to in Section12.9 approved by the P AO.

4.1.6 The applicant CA shall have implemented an Information Security Management System in accordance with ISO/IEC27001. However, the CA must be ISO/IEC 27001certified by the time it applies for the first renewal of its accreditation.

4.1.7 The applicant shall undergo an initial assessment before an accreditation certificate can be granted by the PAO. The assessment shall consist of the following:

4.1.7.1. Documentation Review- the CPS and associated documents shall be reviewed by the Lead Assessor and/or Team Leader, in order to verify if the applicant CA addresses all the requirements of the relevant standards and PAO requirements.

4.1.7.2. Pre-assessment visit - This process shall be conducted if it is requested by the applicant CA. The nominated assessment team and normally those who conducted the documentation review shall conduct the pre-assessment. The management system, quality documentation and its implementation shall be discussed during the pre-assessment

4.1.7.3. lnitial assessment - an initial assessment shall be scheduled by the Lead Assessor and/or Team Leader when the non-conformities raised during documentation review and pre-assessment visit have been corrected. The nominated assessment team shall conduct complete assessment of the organizational structure, operation and procedures of the applicant CA.

The initial assessment hall include all other premises of the CA from which one or more key activities are performed. The key activities included are policy formulation, process and/or procedure development and as appropriate, contract review, planning conformity assessments, review, approval and decisions on the results of conformity assessments.

4.1.7.4. Follow-up visit - when required, the Lead Assessor and/or Team Leader shall arrange a follow-up visit to verify corrective actions on any non-conformity raised.

4.2. Financial Criteria

4.2.1. The applicant shall have a minimum paid-up capital of two hundred million pesos (PhP200M); and

4.2.2. The applicant shall be insured against liability for damages inflicted on subscribers while providing certification services in violation of the Electronic Commerce Act, its lmplementing Rules and Regulations or provisions of this Order.

4.2.3. Other documents or proof of financial visability as may be required by PAO.

4.3 Technical Criteria

4.3.1. Facilities and Equipment

4.3.1.1. The facility necessary for managing registered information about subscribers;

4.3.1.2. The facility necessary for creating and managing digital signature creation information and digital signature verification information;

4.3.1.3.The facility necessary for creating ,issuing and managing accredited certificates;