

DEPARTMENT ADMINISTRATIVE ORDER NO. 10-09
SERIES OF 2010

**SUBJECT: 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 Implementing Rules and Regulations, and the provisions of Executive Order No. 810 issued on 15 June 2009 and entitled, "Institutionalizing 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. **"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.
 - 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 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.
- 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 may be 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 signer's 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 Office.
- 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 shareholder"** – in relation to an applicant, which is a company, means a person who owns or controls the voting rights to 10 percent 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 identification of 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 DTI, 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 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 a 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 to 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 (ICT) 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 may be 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 found 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 recommendations made by the assessment team.

4. Conditions for Accreditation

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 Section 12.9 approved by the PAO.

4.1.6. The applicant CA shall have implemented an Information Security Management System in accordance with ISO/IEC 27001. However, the CA must be ISO/IEC 27001 certified 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.

GR M

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. Initial 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 shall 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 (PhP 200M); 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 Implementing Rules and Regulations, or provisions of this Order.

4.2.3. Other documents or proof of financial viability 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;

4.3.1.4. The facility necessary for confirming the date and time when a digital document submitted to an accredited CA.

4.3.1.5. The protective facility necessary for safely operating facilities and equipment used for certification services.

4.3.1.6. The facility necessary for providing certification services by accredited CAs to their subscribers.

4.3.2. Personnel

4.3.2.1. A CA shall have at least seven (7) full-time technical personnel to operate facilities and equipment used for its certification services. At least one (1) shall be a full-time certified information security professional whose certification is issued by the national government or internationally-recognized (ISO 17024) bodies such as, but not limited to, ISACA; SysAdmin, Audit, Network, Security (SANS); and International Information Systems Security Certification Consortium, Inc. (ISC)². The certified information security professional shall oversee the operations/management of the CA.

4.3.2.2. Technical personnel shall have the following qualifications:

4.3.2.2.1. Diploma in computer engineering, computer science or information and communications technology; government-issued license in electronics engineering; and certification in advanced courses on computer science, information and communications technology, electronics engineering or computer engineering, and other related/special courses.

4.3.2.2.2. Work experience of at least five (5) years in the field of information security or operation and management of information and communications technology.

4.3.2.2.3. Not an undischarged bankrupt person in the Philippines or elsewhere, or has made arrangement with his creditors; and

4.3.2.2.4. Has not been convicted, whether in the Philippines or elsewhere, of an offense, the conviction for which involved a finding that he acted fraudulently or dishonestly, or

4.3.2.2.5. An offense under the Electronic Commerce Act or this Order.

4.3.2.3. Every trusted person shall:

4.3.2.3.1. Have a good knowledge of the Electronic Commerce Act and this Order;

4.3.2.3.2. Be trained in the CA's Certification Practice Statement.

4.4. Assessment Requirements

4.4.1. The following shall be assessed on-site to determine actual implementation by the CA:

4.4.1.1. Security guidelines as referred to in Section 12.11;

4.4.1.2. Accreditation criteria as referred to in Section 4; and

4.4.1.3. Its Certification Practice Statement as referred to in Section 12.9.

- 4.4.2. All assessments shall be conducted by a qualified independent assessment team organized by the PAO for this purpose, comprising of, but not limited to, Certified Public Accountants and Certified Information Security practitioners, who possess sufficient knowledge on digital signatures, digital certificates, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Electronic Commerce Act and Executive Order No. 810, among others.
- 4.4.3. Any member of the assessment team and the firm/s or company/ies the member is affiliated with shall have no conflict of interest with the CA being assessed, and shall not be a software or hardware vendor that is or has been providing services or supplying equipment to the CA within the last two (2) years.
- 4.4.4. Assessment fees, as specified in Annex A, shall be borne by the CA.
- 4.4.5. A copy of every assessment report shall be submitted to PAO within four (4) weeks after completion of an assessment.
- 4.4.6. An accreditation panel of three (3) members shall review the assessment reports based on the evidences gathered and will give a recommendation to the head of the PAO whether to accredit or not an applicant CA.

5. Application for Accreditation

- 5.1. The CA applying for accreditation shall be duly registered and operating in accordance with Philippine laws.
- 5.2. Application shall be made in an official form as may be secured from the PAO upon payment of application fee specified in Annex A.
- 5.3. Every application to be an accredited CA shall be made in such form and manner as the PAO may, from time to time, determine, and shall be supported by such information as the PAO may require.
- 5.4. The PAO may require the applicant to furnish such additional information as may be necessary in support of the application.
- 5.5. The PAO may allow applications for renewal of certificates to be submitted in the form of digital records subject to such requirements as the PAO may impose.
- 5.6. A certificate of accreditation shall be subject to such conditions, restrictions, and limitations as the PAO may, from time to time, determine.

6. Renewal of the Accreditation Certificate

- 6.1. Section 6 shall apply to an application for renewal of an accreditation certificate as it applies to a new application for accreditation.
- 6.2. The CA shall submit an application for the renewal of its accreditation certificate not later than six (6) months before the expiry of its accreditation certificate.
- 6.3. If the CA has no intention to renew its accreditation certificate, it shall –

- 6.3.1. Inform the PAO in writing not later than three (3) months before the expiry of the accreditation certificate;
- 6.3.2. Inform all its subscribers in writing not later than two (2) months before the expiry of the accreditation certificate;

7. Grounds for Refusal to Grant or Renew the Accreditation Certificate

PAO shall refuse to grant or renew an accreditation certificate if:

- 7.1. The CA has not provided PAO with information relating to its operations and personnel, and any circumstances which may likely affect its method of conducting business, as PAO may require;
- 7.2. The CA or its substantial shareholder is in the process of winding up or liquidation and dissolution;
- 7.3. A receiver, or a receiver and manager, has been appointed to the CA or its substantial shareholder;
- 7.4. The CA or its substantial shareholder has, whether in the Philippines or elsewhere, entered into a compromise or scheme of arrangement with its creditors that is still in operation;
- 7.5. The CA or its substantial shareholder or any trusted person has been convicted, whether in the Philippines or elsewhere, of an offense the conviction for which involved a finding that it or he acted fraudulently or dishonestly, or has been convicted of an offense under the Electronic Commerce Act or this Order;
- 7.6. The CA has failed to prove that any trusted person has the qualifications or experience to perform duties in connection with the holding of the accreditation certificate by the CA based on the PAO accreditation criteria;
- 7.7. The PAO is not satisfied as to the financial standing of the applicant or its substantial shareholder;
- 7.8. The PAO is not satisfied as to the record of past performance or expertise of the applicant or its trusted person having regard to the nature of the business of, which the applicant may carry on in connection with the holding of the accreditation certificate;
- 7.9. There are other circumstances, which are likely to lead to the improper conduct of business by, or reflect discredit on the method of conducting the business of, the applicant or its substantial shareholder or any of the trusted persons; or
- 7.10. The PAO has the evidence that the granting of the certificate to the CA is not in the interest of the public.

8. Terms and Conditions of the Accreditation Certificate and Use of the Accreditation Symbol

- 8.1. An accreditation certificate shall be valid for three (3) years.
- 8.2. The accredited CA shall be subjected to a yearly surveillance visit within the validity period of the certificate.

- 8.3. The accredited CA shall comply at all times with relevant accreditation criteria and other requirements under this Order.
- 8.4. During assessment, the accredited CA shall allow the assessors access to its premises, facilities, records, and personnel.
- 8.5. The accredited CA shall pay all the required fees as specified in Annex A.
- 8.6. The accreditation certificate is non-transferable, and is valid only for a specific scope of accreditation.
- 8.7. The PAO shall operate a third party symbol for use by its accredited CA. The symbol shall, however, remain the property of PAO.
- 8.8. The symbol may be used by the accredited CA under the terms and conditions of the PAO accreditation scheme.
- 8.9. The accredited CA shall inform the PAO of relevant changes in the following areas that may affect its operations:
 - 8.9.1. Organizational status including trusted persons;
 - 8.9.2. Certification Practice Statement (CPS);
 - 8.9.3. Security Programs Related to CA Operations and Guidelines; and
 - 8.9.4. Any other relevant documents as maybe identified by PAO.

9. Suspension or Revocation of the Accreditation Certificate

- 9.1. The PAO shall suspend the accreditation certificate for a period of 30 days on any of the following grounds:
 - 9.1.1. If the CA fails to comply with the procedures of the PAO accreditation scheme defined in this order;
 - 9.1.2. If the CA fails to disclose that it has entered into any compromise agreement with its creditors;
 - 9.1.3. If the PAO has evidence to prove that the CA or its trusted person has committed misconduct in the performance of its/his duties; and
 - 9.1.4. If the CA contravenes or fails to comply with any condition or restriction applicable in respect to the accreditation certificate
- 9.2. The PAO shall revoke the accreditation certificate on the following grounds:
 - 9.2.1. If the CA fails to correct the non-compliance within the suspension period of 30 days;
 - 9.2.2. If the PAO has evidence to prove that the CA or its trusted person has committed serious misconduct in the performance of its/his duties; and

9.2.3. The PAO shall not suspend or revoke the accreditation certificate on the grounds provided above without first giving the CA an opportunity to be heard.

9.3. Discontinuance of Accreditation

9.3.1. The CA may request to discontinue its accreditation with PAO as deemed necessary.

10. Effect of Suspension or Revocation of the Accreditation Certificate

10.1. For purposes of this Order, a CA, whose accreditation certificate is suspended or revoked under Section 9, shall be deemed not accredited from the date that the PAO suspends or revokes the certificate, as the case may be.

10.2. A suspension or revocation of an accreditation certificate of a CA shall not –

10.2.1. Avoid or affect any agreement, transaction or arrangement entered into by the CA prior to the suspension or revocation of the accreditation certificate; or

10.2.2. Affect any right, obligation or liability arising under any such agreement, transaction or arrangement.

11. Appeal

11.1. A CA may file an appeal to the PAO Council based on the following:

11.1.1. Refusal of PAO to grant or renew an accreditation certificate under Section 7, or

11.1.2. When PAO suspends or revokes an accreditation certificate under Section 9.

11.2. Period to Appeal

11.1.1. A CA may file an appeal to the PAO Council, copy furnished the PAO, within 15 days from receipt of a copy of the refusal, suspension or revocation.

11.1.2. The PAO Council will render a decision on an appeal filed within 30 days after filing.

12. Conduct of Business by the Accredited Certification Authority

12.1. An accredited CA must comply with the requirements of ISO/IEC 27001.

12.2. Trustworthy Record Keeping and Archival

12.2.1. An accredited CA shall keep its records in the form of paper-based documents, digital records, or any other form approved by the PAO.

12.2.2. Such records shall be indexed, stored, preserved, and reproduced so as to be accurate, complete, legible, and accessible to the PAO assessment team, or technical experts.

12.3. Trustworthy Transaction Logs

- 12.3.1. Every accredited CA shall make and keep in a trustworthy manner the records relating to:
 - 12.3.1.1. Activities in issuance, renewal, suspension, and revocation of certificates (including the process of identification of any person requesting a certificate from an accredited CA);
 - 12.3.1.2. The process of generating subscribers' (where applicable) or the accredited CA's own key pairs; and
 - 12.3.1.3. Such critical related activity of an accredited CA as may be determined by the PAO.
- 12.3.2. Every accredited CA shall archive all certificates issued by it and maintain mechanisms to access such certificates for a period of 10 years from the date of issuance of the certificate.
- 12.3.3. Every accredited CA shall retain all records that are required to be kept under Section 12.3.1, and all logs of the creation of the archive of certificates referred to in Section 12.3.2 for a period of 10 years from the date of issuance of the certificate.

12.4. Issuance of the Certificate

- 12.4.1. An accredited CA may issue a general purpose or specific purpose certificate.
- 12.4.2. Every accredited CA shall comply with the requirements relative to the issuance of certificates.
- 12.4.3. The certificate shall contain, or incorporate by reference, such information as is sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate will be listed if the certificate is suspended or revoked.
- 12.4.4. The accredited CA shall at all times comply with practices and procedures set forth in its CPS.
- 12.4.5. The subscriber identity verification method employed for issuance of certificates shall be specified in the CPS and is subject for approval of the PAO during the application for an accreditation.
- 12.4.6. Where a certificate is issued to a person (referred to in this Order as the new certificate) on the basis of another valid certificate held by the same person (referred to in this Order as the originating certificate), and subsequently the originating certificate has been suspended or revoked, the CA that issued the new certificate shall conduct investigations to determine whether it is necessary to suspend or revoke the new certificate or not.
- 12.4.7. The accredited CA shall provide a reasonable opportunity for the subscriber to verify the contents of the certificate before it is accepted.

- 12.4.8. The accredited CA shall publish a signed copy of the certificate in a repository referred to in Section 12.4.3, unless there is a contractual agreement between the CA and subscriber not to publish the certificate.
- 12.4.9. If the subscriber does not accept the certificate, the accredited CA shall not publish it.
- 12.4.10. Once the certificate has been issued by the accredited CA, and accepted by the subscriber, the accredited CA shall notify the subscriber within a reasonable time of any fact known to the accredited CA that significantly affects the validity or reliability of the certificate.
- 12.4.11. The date and time of all transactions in relation to the issuance of a certificate shall be logged, and kept in a trustworthy manner.

12.5. Renewal of the Certificate

- 12.5.1. Section 12.5 shall apply to the renewal of certificates as it applies to the issuance of certificates.
- 12.5.2. The subscriber identity verification method shall be that specified in the CPS as approved by the PAO.
- 12.5.3. The date and time of all transactions in relation to the renewal of a certificate shall be logged, and kept in a trustworthy manner.

12.6. Suspension of the Certificate

- 12.6.1. This section shall apply only to every accredited CA which allows subscribers to request for suspension of certificates.
- 12.6.2. Every accredited CA may provide for immediate revocation instead of mere suspension if the subscriber has agreed in writing.
- 12.6.3. Upon receiving a request for suspension of a certificate, the accredited CA shall ensure that the certificate is suspended, and notice of the suspension published in the repository.
- 12.6.4. An accredited CA may suspend a certificate that it has issued if it has reasonable grounds to believe that the certificate is unreliable, regardless of whether the subscriber consents to the suspension or not; but the accredited CA shall complete its investigation into the reliability of the certificate, and decide within a reasonable time whether to reinstate or to revoke the certificate.
- 12.6.5. It is the responsibility of any person relying on a certificate to check whether a certificate has been suspended or not.
- 12.6.6. An accredited CA shall suspend a certificate after receiving a valid request for suspension; but if the accredited CA considers that revocation is justified in the light of all the evidence available to it, the certificate shall be revoked.
- 12.6.7. An accredited CA shall check with the subscriber or his authorized agent whether the certificate should be revoked or not and whether to reinstate the certificate after suspension or not.

- 12.6.8. An accredited CA shall terminate a suspension, initiated by request if it discovers and confirms that the request for suspension was made without authorization by the subscriber or his authorized agent.
- 12.6.9. If the suspension of a certificate leads to a revocation of the certificate, the requirements for revocation shall apply.
- 12.6.10. The date and time of all transactions in relation to the suspension of certificates shall be logged, and kept in a trustworthy manner.
- 12.6.11. An accredited CA shall maintain facilities to receive and act upon requests for suspension at all times of the day, and on all days of every year.

12.7. Revocation of the Certificate

A CA shall revoke the certificate that it issued –

- 12.7.1. After receiving a request for revocation by the subscriber named in the certificate, and confirming that the person requesting the revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation;
- 12.7.2. In order to confirm the identity of the subscriber or authorized agent making a request for revocation, the accredited CA shall use the subscriber identity verification method specified in the CPS for this purpose;
- 12.7.3. After receiving a certified copy of the subscriber's death certificate or upon confirming by other evidence that the subscriber is dead;
- 12.7.4. Upon presentation of documents effecting dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.
- 12.7.5. Immediately upon revocation of a certificate by an accredited CA, the CA shall publish a signed notice of the revocation or a Certificate Revocation List (CRL) in the repository specified in the certificate for publication of notice of revocation.
- 12.7.6. Where one or more repositories are specified, the accredited CA shall publish signed notices of the revocation/CRL in all such repositories.
- 12.7.7. An accredited CA shall maintain facilities to receive and act upon requests for revocation at all times of the day, and on all days of every year.
- 12.7.8. An accredited CA shall give notice to the subscriber immediately upon the revocation of the certificate.
- 12.7.9. The date and time of all transactions in relation to the revocation of certificates shall be logged, and kept in a trustworthy manner.

12.8. Validity Period of the Certificate

- 12.8.1. A certificate shall be valid for one (1) year. The expiry date shall be clearly indicated in the certificate.

12.9. Certification Practice Statement (CPS)

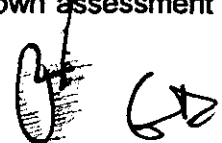
- 12.9.1. Every accredited CA shall use the current edition of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, as a guide for the preparation of its CPS.
- 12.9.2. Any change to the CPS during the term of the accreditation requires the prior approval of the PAO.
- 12.9.3. Every accredited CA shall highlight to its subscribers any limitation of their liabilities and in particular, it shall draw the subscriber's attention to the implication of reliance limits on their certificates.
- 12.9.4. The subscriber identity verification method for the issuance, suspension, revocation, and renewal, of a certificate shall be specified in the CPS.
- 12.9.5. A copy of the latest version of the CPS, together with its effectivity date, shall be filed with the PAO, and published on the CA's Internet website accessible to members of the public.
- 12.9.6. After the effectivity date, the latest version filed with the PAO will be the prevailing version for a particular certificate.
- 12.9.7. Every accredited CA shall log all changes to the CPS, together with the effective date of each change.
- 12.9.8. An accredited CA shall keep in a trustworthy manner a copy of each version of the CPS, together with the date it came into effect and the date it ceased to have effect.

12.10. Digital Signatures

- 12.10.1. The technical implementation of the requirements specified by PAO shall be to ensure that it shall not be feasible, by computation or by any other means, for any person other than the person to whom the signature correlates to have created a digital signature, which is verified by reference to the public key listed in that person's certificate.
- 12.10.2. The digital signature on its own should be such as to –
 - 12.10.2.1. The steps taken towards the creation of the signature shall be under the direction of the person to whom the signature correlates, and
 - 12.10.2.2. No other person can reproduce the sequence of steps to create the signature and thereby create a valid signature without the involvement or the knowledge of the person to whom the signature correlates.

12.11. Security Guidelines

- 12.11.1. Every applicant/accredited CA shall ensure that in the performance of its services, it complies with the requirements of ISO/IEC 27001.
- 12.11.2. Notwithstanding an auditor's assessment of whether a departure from the security guidelines is material or not, the PAO may make its own assessment



and reach a conclusion for the purpose of Section 12.11.1 which is at variance with that of the auditor.

- 12.11.3. Every accredited CA shall provide every subscriber with a trustworthy system to generate his key pair.
- 12.11.4. Every accredited CA shall provide the mechanism to generate and verify digital signatures in a trustworthy manner, and the mechanism provided shall also indicate the validity of the signature.
- 12.11.5. If the digital signature is not valid, the mechanism provided should indicate if the invalidity is due to the integrity of the document, or the signature and the mechanism provided shall also indicate the status of the certificate.
- 12.11.6. For mechanisms provided by third parties other than the accredited CA, the resulting digital signature is considered secure only if the accredited CA endorses the implementation of such mechanism in conjunction with its certificate.
- 12.11.7. Every accredited CA shall be responsible for the storage of keys (including the subscriber's public key and the accredited CA's own key) in a trustworthy manner.

12.12. Incident Handling

- 12.12.1. An accredited CA shall implement an incident management plan that shall provide at least for management of the following incidents:
 - 12.12.1.1. Compromise of CA's signing key;
 - 12.12.1.2. Penetration of CA's system and network;
 - 12.12.1.3. Unavailability of infrastructure; and
 - 12.12.1.4. Fraudulent registration and generation of certificates, certificate suspension and revocation information.
- 12.12.2. If any incident referred to in Section 12.12.1 occurs, the accredited CA shall report it to the PAO within the next working day.

12.13. Confidentiality

- 12.13.1. An accredited CA must comply with the requirements of ISO/IEC 27001.
- 12.13.2. Every accredited CA and its authorized agent shall keep all subscriber-specific information confidential except as required by law, or pursuant to an order of court.
- 12.13.3. Any disclosure of subscriber-specific information by the accredited CA or its agent shall be authorized by the subscriber.
- 12.13.4. This Order shall not apply to subscriber-specific information, which –
 - 13.13.4.1. Is contained in the certificate for public disclosure;

13.13.4.2. Is otherwise provide by the subscriber to the accredited CA for this purpose; or

13.13.4.3. Relates to the fact that the certificate has been revoked or suspended.

12.14. Protection of Personal Information

12.14.1. Accredited CAs shall conform to the provisions of DTI Department Administrative Order No. 8, issued on 21 July 2006 and entitled "Prescribing Guidelines for the Protection of Personal Data in Information and Communications System in the Private Sector."

12.15. Change in Management

12.15.1. An accredited CA shall inform the PAO of any changes in the appointment of any person as its director or chief executive, or of any person to perform functions equivalent to that of a chief executive within three (3) working days from the date of appointment of that person.

13. Availability of General Purpose Repository

13.1. A general-purpose repository shall be made available at all times of the day, and on all days of every year.

13.2. A general-purpose repository shall have an aggregate uptime not less than 99.7% (or aggregate downtime not exceeding 0.3%) at any period in one (1) month.

13.3 Any downtime, whether scheduled or not, shall not exceed 30 minutes duration at any one time.

14. Specific Purpose Repository

14.1. Subject to the approval of the PAO, a repository may be dedicated for a specific purpose for which specific hours of operation may be acceptable.

15. Application to Government and Statutory Corporations

15.1 All departments of the Government, organs of State or statutory corporations that seek to apply as a CA shall comply with the provisions of this Order with the exception of Section 4.2.1.

15.2 The provisions referred to in Section 15.1 shall be subject to necessary and other modifications as the PAO may determine to be applicable to the department of the Government, organ of State or statutory corporations.

16. Disclosure

16.1. The accredited CA shall submit a semi-annual progress report and audited annual financial statements to the PAO.

Handwritten initials/signature

- 16.2. The semi-annual progress reports shall include information on –
- 16.2.1. The number of subscribers;
 - 16.2.2. The number of certificates issued, suspended, revoked, expired and renewed;
 - 16.2.3. System performance including system up and down time and any extraordinary incidents;
 - 16.2.4. Changes in the organizational structure of the CA;
 - 16.2.5. Changes since the preceding progress report submitted or since the application for the accreditation; and
 - 16.2.6. Changes in the particulars of any trusted person since the last submission to the PAO, including the name, identification number, residential address, designation function, and date of employment of the trusted person.
- 16.3. The accredited CA has a continuing obligation to disclose to the PAO any changes in the information submitted.
- 16.4. All current versions of the accredited CA's applicable CPS together with their effective dates shall be published in its Internet web site.

17. Suspension or Termination of Certification Service/Discontinuation of Operations of Accredited Certification Authority

17.1. Suspension of Certification Service

- 17.1.1. An accredited CA that intends to suspend all or part of its certificate service shall notify its subscribers in writing of the suspension period no later than 30 days before such intended suspension.
- 17.1.2. The accredited CA shall likewise file a written notice/report with PAO no later than 30 days before the intended suspension.
- 17.1.3. The suspension period shall not exceed six (6) months.

17.2. Termination of Certification Service/Discontinuation of Operations

- 17.2.1. If an accredited CA intends to terminate its certification service or discontinue its operations, it shall arrange for its subscribers to re-subscribe to another accredited CA.
- 17.2.2. The accredited CA shall make arrangements for its records and certificates to be archived in a trustworthy manner.
- 17.2.3. If the records are transferred to another accredited CA, the transfer shall be done in a trustworthy manner.
- 17.2.4. Should arrangements for re-subscription/transfer of records and certificates not be effected due to unavoidable circumstances, the accredited CA shall file a report with PAO.



- 17.2.5. Upon receipt of the report of the inability to assign/transfer as stated in Section 17.2.4, PAO may request the Government CA to take over the subscriber certificates, records, etc. from the accredited CA, and manage said certificates.
- 17.2.6. The accredited CA shall notify its subscribers in writing no later than 60 days before the date of termination/discontinuation of operations.
- 17.2.7. It shall likewise give PAO a minimum of 90 days' written notice of its intention to terminate its certification service or discontinue its operations.
- 17.2.8. It shall advertise its intention in a daily newspaper of general circulation, and in a manner as the PAO may determine, no later than 60 days before the date of termination of its certification service/discontinuation of its operations.


18. Separability Clause

In the event that any of the provisions of this Order is declared invalid or unconstitutional, all the provisions not affected thereby shall remain valid and in effect.

19. Effectivity

This Order shall take effect on the 15th day after publication of its full text in the Official Gazette or in one (1) newspaper of general circulation.

Recommending Approval:


ZENAIDA GUISON MAGLAYA
Undersecretary for Consumer Welfare
and Trade Regulation


ATTY. ADRIAN S. CRISTOBAL, JR.
Undersecretary for International Trade

Approved:


GREGORY L. DOMINGO
Secretary

Date: 29 September 2010

Schedule of Fees

1. The following fees (in Philippine pesos) shall be collected by PAO from its Accredited Certification Authorities (CAs) and prospective/applicant CAs:
 - 1.1. Application Fee (initial and renewal) 10,000.00
 - 1.2. Assessment Fees (initial, surveillance and renewal)
 - 1.2.1. Certified Public Accountant (CPA)/
Certified Information Systems Security Professional (CISSP)/
Certified Information Security Auditor (CISA) 3,000.00/manhour
1,000.00/manhour
 - 1.2.2. PAO Assessor
 - 1.3. Initial Accreditation Fee (payable upon issuance of certificate) 50,000.00
 - 1.4. Renewal Fee 40,000.00
 - 1.5. Annual Fee 30,000.00
2. The CA shall pay the contracted assessors/experts through PAO based on the above assessment fees.
3. Transportation expenses and hotel accommodation of assessment team on official business shall be borne by the prospective/applicant/accredited CA.
4. The PAO shall not refund any fee paid if the application is not approved, withdrawn or discontinued or if the Certificate is suspended or revoked.

612
M