[ICTO MEMORANDUM CIRCULAR NO. 2014-001, April 25, 2014]

PRESCRIBING POLICIES AND PROCEDURES GOVERNING THE ACCREDITATION OF GOVERNMENT REGISTRATION AUTHORITIES UNDER THE NATIONAL CERTIFICATION SCHEME FOR DIGITAL SIGNATURES

Adopted: 25 April 2014
Date Filed: 02 July 2014

Pursuant to 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 Memorandum Circular is hereby prescribed by the National Computer Center (NCC), in its capacity as Government Certification Authority (GovCA), for the compliance, information, and guidance of all concerned:

Section I OBJECTIVES

This Memorandum Circular prescribes the POLICIES AND PROCEDURES governing the accreditation of government agencies as Government Registration Authorities (GovRAs) under the National Certification Scheme for Digital Signatures as mandated under Executive Order No. 810, Series of 2009.

Section II DEFINITION OF TERMS

1. **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), under the Department of Trade and Industry (DTI);
2. **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;
3. **General Certificate** - a certificate which can be used for all government and private transactions;
4. **Specific Purpose Certificate** – a certificate which can only be used for specific purpose;
5. **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;
6. **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;

7. **Digital Signature** - refers to an electronic signature consisting of a transformation of an electronic document of an electronic data message using an asymmetric or public cryptosystem, such that a person having the initial untransformed document and the signers 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;
8. **Government Certification Authority (GovCA)** - refers to the government body that 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. The GovCA designates Government Registration Authorities (GovRAs) and conducts regular assessment of such GovRAs to ensure compliance to prescribed criteria, guidelines and standards. The GovCA is part of the lCT Office;
9. **Government Registration Authority (GovRA)** - refers to a government agency designated by the Certification Authority (CA) to perform administrative tasks such as end-user registration;
10. **Root Certification Authority (Root CA)** - issues and manages certificates to government and private CAs; the Root CA is part of the ICT Office;
11. **Subscriber** - an individual or entity applying for and using digital certificates issued by the CA;
12. **Personal Information Controller** - means a person or organization that controls the collection, holding, processing or use of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer; or disclose personal information on his or her behalf, but excludes a person or organization that performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

Section III GOVERNMENT REGISTRATION AUTHORITY ACCREDITATION

GovRA accreditation is granted following the mandatory evaluation of an applicant-government agency's compliance with this Circular. Certification shall be valid for three (3) years, unless suspended or revoked sooner, and subject to the mandatory annual assessment of compliance.

Section IV CONDITIONS FOR ACCREDITATION FOR GOVRA

1. Certification shall be valid for three (3) years unless suspended or revoked sooner, and subject to the mandatory annual assessment of compliance;

2. The GovRA-applicant must fulfill basic technical agency requirements before or during the certification process. The full list of technical agency-related requirements is attached as Annex A, which shall form an integral part of this Memorandum;

3. *Application for accreditation*

(a) The GovRA-applicant shall send an application letter to the GovCA outlining their objectives in applying for the position of GovRA and their intended subscribers;

(b) On receipt of the application letter and the accomplished application form, the GovCA shall acknowledge the application within nine (9) calendar days and direct the applicant-government agency to complete the following required documents within thirty (30) calendar days for document review. The required documents shall form part of the criteria used to evaluate the applicant-agencies, and shall be discussed in detail on Article V:

i. Certified copy of charter/legal document creating the agency and any amendments;
ii. Disaster recovery and business continuity plan;
iii. GovRA operations manual;

(c) If the GovRA-applicant is not able to respond to submission of the required documents within the specified number of days stated above, the processing of the application shall be terminated. However, the GovRA-applicant may still reapply for GovRA accreditation;

4. *Document Review*

(a) The GovCA shall undertake the review of the submitted documents. Results of the review are communicated to the GovRA-applicant for any clarifications or concerns regarding the submitted documents;

(b) The GovRA-applicant must address the concerns raised by the document reviewer within five (5) days. All the required documents need to be approved before an applicant government agency is accredited as a GovRA.

5. *Preparation for Assessment*

(a) An assessment team shall be appointed by the GovCA to conduct an onsite assessment of the GovRA-applicant premises;

(b) The assessment team shall sign an Impartiality and Confidentiality Statement before conducting the assessment;

6. *Conduct of Assessment*

(a) The date of assessment shall be communicated to the GovRA-applicant prior to the actual assessment and shall be agreed upon by the GovRAapplicant and the GovCA;

(b) The assessment shall be done against the requirements of relevant standards and criteria as required by GovCA;

(c) During the assessment, the team shall review the policies and procedures of the GovRA-applicant as documented in its Operations Manual and other relevant documents. The team shall also assess the implementation of these operation standards and the overall competence of the GovRA-applicant in their issuance of digital certificates or signatures;

7. *Evaluation*

(a) Following completion of document review and on-site assessment, an evaluation shall be conducted by an independent panel assigned by the GovCA;

(b) All costs involved in the course of the assessment shall be the responsibility of the GovRA-applicant.

8. *Recommendation*

(a) If there are no negative findings raised/ the GovRA-applicant shall be recommended for accreditation. Otherwise, the GovRA-applicant shall be given thirty (30) calendar days to rectify the negative findings. If the GovRA-applicant is unable to remediate the negative findings, the application shall be denied;

(b) A recommendation letter for accreditation will be issued to the successful GovRA-applicant. A Memorandum of Understanding shall be signed between the GovCA and the (recommendee) successful GovRAapplicant, with the final version of the approved documents evaluated during the accreditation process annexed as part of the memorandum.

9. *Issuance of Certificate*

(a) A certificate shall be issued to the successful GovRA- applicant and their information added to the GovCA website;

(b) The whole accreditation process is required to be completed within ninety (90) calendar days from the date of submission of documents, otherwise the GovRA-applicant shall need to re-apply;

(c) The requirements for certification are a continuing requirement that must be maintained by the GovRA-certified agency for as long as it is functioning as such. The GovCA may revoke the agency's GovRA status if the GovRA fails to uphold its requirements.

Section V DOCUMENTARY CRITERIA FOR APPLICANT EVALUATION

Strict compliance with the criteria listed below is mandatory for all government agencies applying for certification to become a GovRA. All approved documents for public use are required to be uploaded and made public to the GovRA website. The following essential documents must be supplied and will be used for evaluation:

1. *Disaster Recovery and Business Continuity Plan*

The Disaster Recovery and Business Continuity Plan is an internal document for the use of GovRA personnel describing how services will be restored in the event of a system crash or failure.

It shall describe the emergency response procedure to be followed in the event of a disaster affecting the functions of the GovRA, a security incident, or suspected security incident affecting the functions of the GovRA. The document shall include mechanisms for the preservation of evidence of system misuse which could be admissible in a court of law.