Republic of the Philippines
Department of Science and Technology
INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE

April 25, 2014

MEMORANDUM CIRCULAR NO. 2014-001
Series 2014

FOR: **GOVERNMENT AGENCIES WANTING TO BECOME A GOVERNMENT REGISTRATION AUTHORITY (GOVRA)**

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

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 a 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 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;

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 ICT 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 on-site 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 GovRA-applicant 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 GovRA-applicant, 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.

This internal document is not publicly available and is restricted to ensure that the document is consistent with the information contained in the Security Profile, Operations Manual and the Code of Practice for Information Security Management (ISO/IEC 27002:2005) and the Guidelines for Information and Communications Technology Disaster Recovery Services (ISO/IEC 24762:2008).

2. *GovRA Operations Manual*

The GovRA Operations Manual describes how the GovRA service will be operated and managed on a day to day basis, providing details of the functions and responsibilities of the personnel within the GovRA. It is essentially an internal document for use by the GovRA staff and will also describe the GovRA staffs' training plan and the Entity Identification process when hiring staff. It will provide directions for the personnel on the implementations of policies and procedures specified in the Security Profile and the Disaster Recovery and Business Continuity Plan.

Section VI PERSONNEL HIRING REQUIREMENTS

The GovRA hiring practices shall include, as a minimum, the following processes on personnel handling Entity Identification materials:

1. Duly accomplished GovRA Employee User Application Form to be submitted to GovCA;
2. Police, NBI and Court Clearance;
3. Background check;
4. Mandatory orientation session with each employee;
5. Computer literate;
6. Signed non-disclosure agreement between the GovRA and the employee;
7. Development and implementation of appropriate training courses for all GovRA employees;
8. Orientation course on Electronic Commerce Act of 2000 (R.A. 8792), Executive Order No. 810, Series of 2009, Data Privacy Act of 2012 (R.A. 10173) and Cybercrime Prevention Act of 2012 (R.A. 10175);
9. Orientation course on GovRA module, including Overview, Configuration and RA User Operation, and GovCA Certificate Policy and Certification Practice Statement (CPS) to be conducted by the GovCA.

Section VII SUBSCRIBER-APPLICANT IDENTIFICATION PROCESSING

Identification of the subscribers of Digital Certificates shall be done through the following:

1. *An individual applicant shall comply with the following for identification:*

   (a) Personal appearance of the applicant;

   (b) Taxpayer Identification Number (TIN);

   (c) A Unified Multi-Purpose Identification (UMID)-compliant card. In the absence of a UMID-compliant card, any two of the following cards are allowed as valid IDs based on BSP Circular 608, series of 2008:

   i. Passport
   ii. Driver's License
   iii. Professional Regulation Commission (PRC) ID
   iv. National Bureau of Investigation (NBI) Clearance
   v. Police Clearance
   vi. Postal ID
   vii. Voter's ID
   viii. Government Service Insurance System (GSIS) e-Card
   ix. Social Security System (SSS) Card
   x. Senior Citizen Card
   xi. Overseas Workers Welfare Administration (OWWA) ID
   xii. OFW ID
   xiii. Seaman's Book
   xiv. Alien Certification of Registration/Immigrant Certificate of Registration
   xv. Government Office and GOCC ID, e.g. Armed Forces of the Philippines (AFP ID), Home Development Mutual Fund (HDMF ID)
   xvi. Certification from the National Council for the Welfare of Disabled Persons (NCWDP)
   xvii. Department of Social Welfare and Development (DSWD) Certification
   xviii. Integrated Bar of the Philippines
   xix. Company IDs Issued by Private Entities or Institutions Registered with or Supervised or Regulated either by the BSP, SEC or Insurance Commission

   (d) A passport-sized photo taken within the last six (6) months;

   (e) Phone number (mobile and/or landline);

   (f) E-mail address owned by the individual or authorized by the owner for use by the subscriber;

(g) Latest copy of a bill or ID showing the physical address of the applicant, where the PIN which will be used to activate a digital certificate shall be mailed; and

(h) Consent to verify the information submitted.

2. *For the juridical applicant:*

(a) Requests for CA certificates shall include the CA name, address and documentation of the existence of the organization;

(b) The PNPKI RootCA or subordinate CA shall verify the information in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA;

(c) A juridical applicant's information shall be verified with prior submission of the following:

i. Taxpayer Identification Number (TIN);
ii. Authorization Letter or Board Resolution naming up to three (3) authorized representative/s to apply for a digital certificate in behalf of the agency;
iii. Consent to verify the information submitted;
iv. Verified e-mail address owned by the organization or authorized by the owner of the e-mail address to be used by the organization; and
v. Latest copy of a bill containing the address of the applicant where the PIN, which will be used to activate a digital certificate, shall be mailed;
vi. Juridical applicants shall send their applications via authorized representatives who shall comply with all of the requirements for individual applicant;

(d) For a government agency:

i. Government Service Insurance System (GSIS) registration number;

(e) For non-government agencies:

i. Securities and Exchange Commission (SEC) business registration for corporation and partnership, DTI Certificate of Business Name Registration for single proprietorship, or Cooperative Development Authority (CDA) registration for cooperatives;
ii. Business Permit issued by the Local Government Unit (LGU); and
iii. Social Security System (SSS) Employer Clearance;

(f) For organizations requesting SSL Certificates, the following requirements shall be complied:

i. Authorization letter, signed by the head of the organization, naming the authorized representative/s; and
ii. Certification from the Philippine Government Internet Domain Name Registry validating the authenticity of the entity's domain name or other recognized domain name registry operating in the Philippines recognized by the PNPKI; or any proof of ownership of a particular domain name.

Section VIII PRIVACY POLICY

The processing of personal information shall be allowed, subject to compliance with the requirements of this Guideline and other laws, in particular R.A. 10173, allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose, and proportionality.

Personal information must be:

1. Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

2. Processed fairly and lawfully;

3. Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

4. Adequate and not excessive in relation to the purposes for which they are collected and processed;

5. Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

6. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing.

The GovRA must ensure implementation of personal information processing principles set out herein.

Section IX AMENDMENTS TO THE GUIDELINES

The accreditation guidelines outlined in this Circular may change over time to reflect advances in technology and government policies. Any such amendments will be done in consultation with existing accredited GovRAs in accordance with the terms of their existing certification. The time frame for compliance with the new criteria is set to ninety (90) days.

Section X OTHER APPLICABLE LAWS AND PENALTIES

The use and issuance of digital certificates shall be covered by the provisions of Republic Act No. 8792 or the Electronic Commerce Act of 2000, Republic Act No. 8484 or the Access Devices Regulation Act of 1998 and Republic Act No. 7394 or the Consumer Act of the Philippines and their Implementing Rules and Regulations (IRRs). Hence, violations committed against such laws in relation to the use and issuance of digital certificates shall be subject to the penalties applicable under said laws and their IRRs.

Section XI DIRECTIVE TO THE DOST-ICT OFFICE RECORDS OFFICER

The DOST-ICT Office Records Officer is hereby ordered to furnish three (3) certified true copies of this Memorandum Circular and the attached annex to the University of the Philippines Law Center.

Section XII EFFECTIVITY

This Circular shall take effect immediately.

Recommending approval:

DENIS F. VILLORENTE
Officer-in-Charge
Office of the Deputy Executive Director for e-Government

Approved by:

LOUIS NAPOLEON C. CASAMBRE
Executive Director
ICT Office

Annex A AGENCY REQUIREMENTS

The following are agency-related requirements that need to be fulfilled as part of applying to be a GovRA.

1. Allowed by their charter/mandate to collect fees
2. Telephone line for voice call and fax, capable of accessing landline and mobile numbers
3. Office space for GovRA operation
4. At least 4 square meters per GovRA Employee User
5. Teller-type enclosure for privacy
6. Working table and chair
7. Chairs for subscribers
8. Adequate power supply and lighting
9. Air-conditioned room
10. Computer system per GovRA Employee User (specifications subject to change as may be deemed necessary by the GovCA)
    - 10.1. CPU 1.8ghz and above
    - 10.2. At least 2GB memory for RAM
    - 10.3. 800x600 display or higher
    - 10.4. Enough storage for operating system and other required applications and utilities
    - 10.5. Internet Connection
    - 10.6. Operating system compatible with the GovRA module
11. Web browser compatible with the GovRA module
12. Anti-virus software
13. USB secure token per GovRA Employee User to be used for accessing the GovRA module
14. Steel filing cabinet with security lock
15. UMID-card reader