GovRA Operations Manual

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
+63 (02) 920 0101

I. Introduction

a. Definition of terms

i. **Subscribers** – an individual or juridical entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the keys and certificate in accordance with the certificate policy;

ii. **Certificate Policy (CP)** – a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements;

iii. **Certificate Practice Statement (CPS)** – a document that contains a detailed description of the practices followed by the GovCA in issuing and managing certificates. In general, the CPS also describes practices relating to all certificate life cycle services;

iv. **Domain** – refers to the group of subscribers serviced by the GovRA;

v. **Token** – refers to a tangible device that contains the digital certificate and allows the subscriber to carry the digital certificate and use it to verify and sign documents, or access and log-in to secure systems under the PKI;

vi. **Web Manage**r – refers to the user interface that a Systems Administrator or GovRA Administrator uses to process subscribers' digital certificate requests.

b. Systems Overview

A GovRA Unit is a component of the Issuing GovCA that collects and processes subscriber applications for digital certificates. It comprises both personnel and web-based tools. The GovRA manages the life cycle of the application process.

c. Basic Functions

i. Identify the users and register the users' information;
ii. Process issuance, revocation, suspension, and modification requests.

d. **Roles and Responsibilities.** The following are the key positions within a GovRA unit.

i. **Auditor**. The GovRA Unit shall have an internal and external auditor as a check and balance mechanism to ensure integrity of GovRA operations. External auditors shall be independent third party auditors who shall conduct a minimum of one (1) audit a year over the GovRA operations.

1. Shall use access logs generated from the GovRA system, as well as other reports or documentation, to determine whether the agency GovRA complies with all pertinent rules and regulations;
2. Shall submit its audit report to the head of the GovRA unit and the GovCA. The audit report shall be used in determining the GovRA's accreditation status;
3. Shall promote the integrity of data collection, processing, and storage, as well as the GovRA Unit's fidelity to security controls and procedures.

ii. **Systems Administrator**

1. Shall receive domain access from the GovCA;
2. Shall be the central point of contact at the GovRA unit's organization for GovRA-related technical issues;
3. Shall maintain the operations of the work stations and PKI-related systems;
4. Shall monitor and maintain the use of the network systems;
5. Shall be authorized to install, configure and maintain trustworthy systems with controlled access to security-related information;
6. Shall provide technical support and troubleshooting for the GovRA administrators of the GovRA unit;
7. Shall function as a system administrator solely for the GovRA unit within an agency.

iii. **GovRA Administrator**. There shall be at least three (3) GovRA administrators for each GovRA unit.

1. Shall accept and verify subscribers' digital certificate application and enrolment;
2. Shall accept and verify subscribers' requests for revocation and suspension;
3. Shall conduct the digitization and encoding of applications;
4. Shall approve certificate applications and requests for revocation and suspension.

iv. Facility Security Officer (FSO)

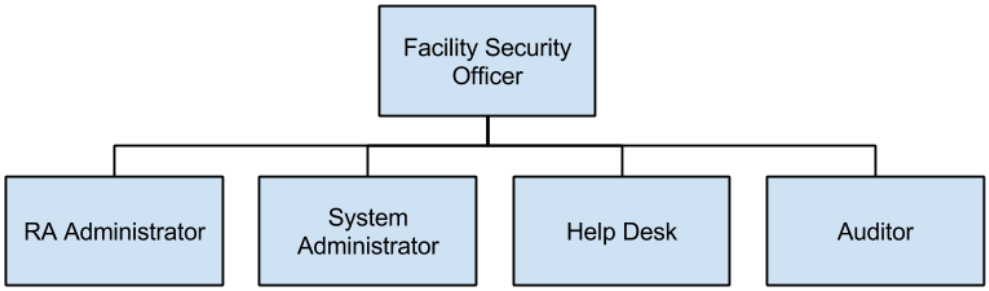
1. Shall maintain the physical and procedural security of the GovRA unit;
2. Shall have overall responsibility for administering the implementation of the security policies and practices;
3. Shall ensure that all the security procedures found in the GovRA Operations Manual, CP, CPS, and other standards and documents pertaining to the operations of the GovRA unit shall be implemented;

4. Shall conduct security audits on a monthly basis, which shall include a check of all security logs, including the logs of the security personnel;
5. Shall be notified of any breach in security, whether physical or procedural. The FSO, in coordination with the System Administrator, shall address security breaches.

v. **Help Desk**

1. Shall answer all questions regarding the application and requests for digital certificates, including in-office visits from applicants, phone calls, and electronic or paper mail sent to the office;
2. May act as the public relations officer representing the GovRA unit in promotional and related events;
3. May assist verification of users during certificate enrollment.

e. Organizational Structure Planning.



II. Applications and Requests

a. Types of application requests:

i. Application for digital certificate;
ii. Request for revocation or suspension.

b. Limits to applications and requests:

i. Digital certificates shall be issued only for appropriate certificate usage which must be lawful, exercised in good faith, and for the intended purposes of a digital certificate;
ii. Limitations on applications and requests include the appropriateness of the use of the certificate for any given purpose. Such purpose must not be prohibited by the CP;
iii. Certificates must be used in accordance with its key-usage field extensions;
iv. The certificate is valid at the time of reliance by reference to an online certificate status protocol or CRL checks;

v. Relying parties are required to seek further independent assurances before any act of reliance is deemed reasonable.

c. Certificate Application Process

i. The applicant shall fill up the application form, which shall be available at the GovRA Units and may be downloaded at _____;
ii. The applicant shall attach all relevant documents to the application form, which shall include:

1. For individual applicants:

a. Personal appearance of the applicant;
b. Tax Payer Identifier Number (TIN);
c. Present a Unified Multipurpose Identification (UMID)-compliant card;
d. Submit a passport-sized photo taken within the last six (6) months;
e. Latest copy of a bill where PIN, to activate the digital certificate, shall be mailed;
f. Phone number;
g. Valid e-mail address;

2. For juridical applicants:

a. For non-government entities, requests for digital certificates shall include the non-government entity's name, address and documentation of the existence of the organization. For corporations, the articles of incorporation shall be required. For others, a business permit, partnership authorization, or baranggay clearance. Juridical applicant's information shall be verified with prior submission of the following:

i. Tax Payer Identification Number (TIN);
ii. Special Power of Attorney/Board Resolution naming up to three authorized representatives;
iii. For a government agency:

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

iv. For non-government entities:

1. Securities and Exchange Commission (SEC) business registration for corporation, DTI Certificate of Business Name Registration for single proprietorship or Cooperative

Development Authority (CDA) registration for cooperatives;
2. Business Permit issued by the Local Government Unit (LGU);
3. Social Security System (SSS) Employer Clearance.

v. Latest copy of a bill where the PIN, to activate the digital certificate, shall be mailed;
vi. Consent to verify the information submitted.

b. For government entities, requests for digital certificates shall include the agency name, address and establishing law or articles of incorporation. Juridical applicant's information shall be verified with prior submission of the following:

i. Tax Payer Identification Number (TIN);
ii. Special Order or Board Resolution naming up to three authorized representatives;
iii. Government Service Insurance System (GSIS) registration number;

3. For authorized representatives:

a. Authorized representatives shall bring all of the above requirements for the individual applicants;
b. With the addition of a special power of attorney or board resolution naming up to three (3) authorized representatives;
c. Any changes in the composition of the authorized representatives must immediately be reported to the GovRA unit, specifying which of the representatives are replaced or retained.

4. For students:

a. Student ID;
b. Certificate of registration;

iii. The fully accomplished application form with the attached documents shall be submitted to the GovRA Administrator. The GovRA administrator shall ensure that all fields in the application form have been filled out and that all the required documents are present;

iv. The GovRA administrator shall verify the information through the following means:

1. TIN, UMID, and present address shall be verified per

application. The GovRA administrator shall counter-check the TIN and UMID numbers with the BIR and UMID-issuing agency's database. Phone numbers submitted shall be called, email address needs response from the user. Board resolution to be verified through the corporate secretary. GSIS, SEC, CDA, LGU, SSS permits or clearances shall be counter-checked with the respective agencies;

2. if any of the submitted information fails verification, the application shall be canceled.

v. The GovRA administrator shall encode the necessary information provided by the applicant into the web manager;
vi. Upon encoding, the GovRA administrator shall add the subscriber into the GovRA system using the web manager;
vii. After adding the applicant, the GovRA administrator shall enroll the user certificate;
viii. Once the applicant has been enrolled, the GovRA Administrator shall approve the enrollment;
ix. The enrolled application shall remain pending within the web manager until two (2) other GovRA administrators approves the application. No application shall be approved by the same GovRA administrator;
x. Upon approval, the subscriber shall be notified via email and a PIN mailer may be generated and sent by the GovRA administrator to the address provided by the subscriber;
xi. The entire process shall not exceed five (5) working days.

d. **Acceptance**

i. Failure of the subscriber to object to the certificate or its contents within five (5) days, after issuance of the certificate, constitutes acceptance of the certificate. The certificate shall be deemed issued once the digital certificate has been downloaded and accessed;
ii. In case of rejection, the subscriber shall apply for revocation of the rejected digital certificate and apply for a new certificate.

e. Renewal, Revocation, Suspension, and Modification Process

i. **Circumstances for Revocation, Suspension Process**

Digital certificate end-users may request for certificate renewal, revocation, suspension, and modification. The request may be coursed through an authorized representative. All complete requests shall be approved.

End-users are encouraged specify the reason for revoking a certificate. By default, the revocation shall be labeled Unspecified. The following are valid reasons that may be selected from the system during revocation:

1. **Key Compromise:** The user's private key was compromised.
2. **CA Compromise:** The key of the Certificate Authority was compromised.
3. **Affiliation Changed**: The user no longer has the affiliation that required the certificate.
4. **Superseded:** The user has a new certificate and does not need this one.
5. **Unspecified:** The user requested a revocation without giving a reason.
6. **Cessation of Operations:** The user no longer needs the certificate for its original use.

ii. Revocation or Suspension Process

1. Revocation requests may only be processed in the GovRA unit issuing the digital certificate in question. In case the GovRA unit no longer exists, the subscriber may forward the request to the GovCA;
2. In case of revocation, the GovCA, GovRA, subscriber or authorized representative may file a request to the GovRA administrator through personal appearance at the GovRA unit, or through phone call, mail, email, or fax. The subscriber or authorized representative must be verified by cross-referencing information previously submitted. The request should indicate the reason for the revocation or suspension, as well as the contact number through which the applicant or representative can be contacted;
3. Requests must be verified. Methods that may be used include:

    a. GovRA Administrator may ask questions cross-referencing the information submitted by the applicant to determine the identity of the subscriber;
    b. GovRA Administrator may use databases, registries and information from government agencies to cross-reference and match the information provided by the subscriber;

4. The GovRA administrator shall issue a report or ticket to the requesting party;
5. The GovRA administrator shall process the request for revocation or suspension through the web manager;
6. The actual revocation must be completed within twenty-four (24) hours;
7. After revocation, the GovRA administrator processing the request shall contact the subscriber and facilitate the filling up of the revocation request form, which must be submitted personally or by an authorized representative of the subscriber within three (3) working days. The revocation request form shall allow the subscriber to obtain a new digital certificate

without having to submit documentary requirements. Subscribers without the revocation request form shall have to submit all required documents and have these verified during application.

II. GovRA Operational Requirements

a. The GovRA unit shall be open for subscriber applications from 8 AM to 5 PM, Monday to Friday;
b. The ICT Office shall act as a centralized GovRA that shall process requests for certificate modification, suspensions, and revocation after office hours, during weekends, and during holidays;
c. Each GovRA unit shall implement a Business Continuity Plan which shall be attached as Annex A of this document;
d. Detailed manuals on how to use the web manager shall be attached as Annex E of this document.

III. Facility Management and Operational Controls

a. **Physical and Security Controls.** The GovRA unit shall implement the following security measures:

i. All computers and other electronic devices used to encode, access or store subscriber information shall be secured with password and must be authenticated with digital certificates;
ii. Hard copies of the documents submitted by applicants and subscribers must be kept in secure, locked cabinets. Logs, minutes, and other documentation related to the operations of the GovRA shall also be secured in the same manner;
iii. The hard copies of documents in the preceding paragraph shall be submitted to the National Archives of the Philippines for proper archiving and disposal, after three (3) years;
iv. The GovRA unit shall be under 24/7 CCTV surveillance and shall regularly be patrolled by security guards, in addition to other security measures in place at the agency where the GovRA is located;
v. All employees, visitors, and guests shall write their name, date of visit, and purpose in a designated log book to be maintained by the Facility Security Officer;
vi. Any technicians, repair crew, service personnel and other third parties must secure authorization from the Facility Security Officer before entering the GovRA unit. Third parties must likewise be accompanied by the facility security officer or a designated officer at all times;
vii. All employees must deposit their personal belongings in a designated locker room. No bags, containers and other personal belongings are allowed inside the working area.

b. **Procedural Controls**

i. Trusted roles

1. Access to the Web Manager shall be determined by the privilege level of the employee. All GovRA personnel that need access to the PKI system are assigned individual accounts with a role attached to access privileges in the system;
2. Certain roles and functions, such as approval, shall be done by separate administrators;
3. No user shall be assigned multiple roles.

ii. Document amendment process

1. The GovRA Manual shall be reviewed by the GovRA Unit and the GovCA annually;
2. Any proposed amendments or changes to the GovRA manual shall be submitted by the GovRA Unit to the GovCA for approval. The GovCA may independently propose amendments or changes to its template manual, which must be applied by the GovRA Unit to its own manual.

iii. Configuration management

1. All hardware, software, and applications used in the GovRA Unit shall be updated by the system administrator. The system administrator shall consult with the GovCA to determine which version to install or implement in the GovRA unit;
2. Only the Web Manager may be installed in the GovRA Unit's workstations. Other applications must be checked by the System Administrator prior to installation. All websites, e-mail, and other applications that allow transfer of data or communication shall be blocked;
3. Computer Administrator Privileges shall be disabled by default by the System Administrator;
4. Only the System Administrator may perform any installation, configuration, or changes in the system;
5. The System Administrator shall routinely perform security checks on the workstations, including virus and malware scans, and installation of security updates.

iv. **Archiving and recovery.** All data and information shall be managed by the GovRA Administrator.

v. Control of removable media

1. The use of removable media, including magnetic media, flash drives, CDs, and other legacy hardware inside GovRA Units shall not be allowed. Security guards shall check personnel for any removal media before coming in or out of the GovRA

premises. All removable media must first be approved and authorized by the System Administrator. Otherwise, the removable media must be deposited with the security guards;
2. The contents of removable media that are brought inside must be scanned by the system administrator before being allowed to leave the facility. No information or data, in part or in whole, from the GovRA systems and databases may be stored or taken outside without prior authorization from the System Administrator. Such authorization must be documented and logged;
3. Unauthorized copying of GovRA-related data shall be grounds for relevant administrative, civil, or criminal action;
4. Any data pertaining to the GovRA Unit authorized to be stored in removable media or taken outside of the office must be digitally signed by the officer taking the data out of the office, for tracking and reference;
5. Third parties authorized to take information or data from the GovRA system, in whole or in part, must sign a confidentiality agreement to be provided by the GovRA unit;
6. A safe or security box shall be used for storing hard tokens used for GovRA operations. The FSO shall have access to the safe or security box. Hard tokens cannot be used outside the GovRA Unit premises, and must be surrendered to the FSO after each shift.

vi. Hiring

1. System Administrators and GovRA Administrators must possess the following qualifications:
    a. Duly accomplished GovRA Employee User Application Form to be submitted to GovCA;
    b. Police, NBI and Court Clearance;
    c. Background check;
    d. Mandatory orientation session with each employee;
    e. Computer literate;
    f. Signed non-disclosure agreement between the GovRA and the employee;
    g. Development and implementation of appropriate training courses for all GovRA employees;
    h. Orientation course on Electronic Commerce Act of 2000 (Republic Act No. 8792) and Executive Order No. 810, Series of 2009;
    i. Orientation course on GovRA module, including Overview, Configuration and GovRA User Operation, and GovCA Certificate Policy and Certification Practice Statement (CPS) to be conducted by the GovCA.
2. Hiring shall be facilitated by the Human Resource Department of the agency to which the GovRA Unit is attached.

vii. **Separation**

1. All personnel working in GovRAs who resign must submit a resignation letter to be approved by the direct supervisor;
2. Upon approval by the direct supervisor, the resigning employee shall be given one (1) month before separating from the unit;
3. An assessment and evaluation of the employee's work shall be conducted. All assigned tasks must be finished, unless the assigned task is not yet due, in which case, only the deliverable milestones, if any, shall be required;
4. The immediate supervisor or a Human Resource Representative shall facilitate an exit interview.

viii. **Audit logging procedures.**

1. The following are auditable events:

    a. **System Access** – the user's certificate serial number will be recorded in the log whenever system access to the GovRA system or web manager is used.
    b. **Physical Access** – Card number and user name shall be logged in for the Physical Access whenever premises or office rooms are used.

2. Audit logs shall be reviewed daily by the Facility Security Officer or the System Administrator. Signed log files are validated to verify the authenticity of the information. Any irregularities, failed validations, or other suspicious activities shall be reported to the Facility Security Officer for further investigation;
3. Digital copies of audit logs shall be kept encrypted and archived permanently;
4. Audit logs shall only be accessible by personnel with the appropriate privilege level. In general, only Auditors, Security Officers, and Systems Administrator shall have access to the audit logs;
5. Any access to audit log files shall automatically be added by the system to the audit logs;
6. Editing and rewriting of audit logs shall not be permitted by the system;
7. Subjects who have caused an audit event shall only be notified of the audit action when the subject is involved in the audit action.

ix. **GovRA Termination**

1. GovRAs shall remain active until mutually agreed upon with the GovCA or upon revocation of the GovRA's accreditation;
2. Upon termination of the GovRA unit, all files, archives, records,

and logs must be forwarded to the GovCA;

3. A public notice announcing the termination of the GovRA Unit must be published in a newspaper of general circulation. This publication shall serve as notice to the subscribers. The notice must include information on where subscribers can file further requests or seek assistance;
4. In the event that a GovRA unit terminates its operation, it shall provide a separate prior notice to the ICT Office, as GovCA, and DTI-PAO prior to termination.

x. **Compliance Audits and Other Assessments.** Auditors shall submit reports detailing the GovRA unit's compliance with the GovRA operations manual, business continuity plan, and other standards imposed by the ICT Office and other authorized bodies.

1. GovRAs must be audited at least annually;
2. GovRAs must have an internal and an external, third-party auditor;
3. A background check shall be enforced upon all auditors to ensure that there are no conflicting business, commercial or other relationship or interest in the matter.

xi. Confidentiality of Information

1. All information provided by subscribers and applicants are considered confidential and may not be shared by the GovRA with any person or agency.
2. Access to subscriber or applicant information shall only be granted upon court warrant.
3. Under no other circumstances may a GovRA disclose any information belonging to an applicant or a subscriber.

Annex A: Business Continuity Plan

Annex B: Diagram of External GovRA functions

Annex C: Password Policy

Annex D: PIN mailer specifications

Annex E: Web Manager Users Manual

INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE
ICTO Building, C.P. Garcia Avenue, Diliman, Quezon City 1101, Philippines
t 63 (02) 920 0101