GPKI Certification Practice Statement
(Root CA CPS)

Version 1.0

2015. 11.

1. OVERVIEW

GPKI Certification Practice Statement is a document of disclosing top-level certification task and certification task policy of GPKI certification system in accordance with the standards of RFC 3647.

GPKI Certification Practice Statement is posted on the website of GPKI Certification Management Center ('hereinafter Certification Management Center').

Institutions or individuals using GPKI personal and institutional certificates can view the GPKI Certification Practice Statement at any time.

This regulation is effective based on October 1, 2015.

1.1 Purpose

The purpose of this regulation is to define specific details in accordance with performance of GPKI certification task and management standards.

1.2 Document name and identification

CA certificates issued by GPKI certification system as follows:

- Ministry of Government Administration and Home Affairs (1.2.410.100001.5.7)
- Ministry of Education (1.2.410.100001.5.3)
- Supreme Prosecutors' Office (1.2.410.100001.5.5)
- Military Manpower Administration (1.2.410.100001.5.6)
- Court (1.2.410.100001.5.8)

1.3 GPKI Certificate System

1.3.1 Root CA (Ministry of Government Administration and Home Affairs)

As a policy supervisory institution for safe and reliable operation of GPKI certification management system, the Ministry of Government Administration and Home Affairs performs the following tasks:

- Policy making for safe, reliable building and operation of GPKI certification management system
- Certification task, consignment of Root CA services, consignment cancellation and notification
- Check the certification task operation status to ensure the safety and reliability of certification task

1.3.2 Certificate Management Center

Certification Management Center is an agency of performing the work of Root CA and

CA of GPKI certification system.

Certification Management Center performs the following tasks.

- Designation of CA and certification task such as CA certificate issuance • management etc.
- Establishment of CA facilities and equipment standards
- Check for safe operation of the facilities and equipment of CA or equivalent measures
- Posting the certificates and certificate revocation list of CA
- Storage of all certificates and certificate revocation lists created by Certification Management Center
- Maintaining information and records related to CA management etc.
- Certification task related education for institutions and subscribers belonging to GPKI certification management system
- Providing mutual linking plan of GPKI Technology Standards and GPKI and authorized electronic signature
- Other tasks related to certification task deemed necessary by Root CA
- Convocation and progress of Certification Association

1.3.3 Certificate Authority

GPKI CA (CA) is an authority left in charge of certification task from the Minister of Government Administration and Home Affairs and designated by notification.

The CA performs the following tasks:

- Designation and management of RA
- Identification of RA and subscribers
- Issuance, renewal, revocation of RA and subscriber certificate and posting of certificate revocation list
- Checking the effectiveness of the certificate issued by the CA
- Maintenance of encryption key consignment • recovery service and related records
- Safe storage, management of records on certification task
- Work deemed necessary as other CA such as point check service etc.

1.3.4 Registration Authority

Registration Authority (RA) left in charge of certification task from administrative . public CA should perform the following tasks:

- Receiving applications and checking applicant identification for certificate issuance, re-issuance, renewal, revocation etc.
- Registration and renewal of subscriber information associated with certificate issuance, re-issuance, renewal, revocation etc.

- Protection of subscriber information
- Safe management of GPKI generating key issued from a certificate authority

1.3.5 Certificate Association

- Certification Association is a consultative body composed to effectively perform certification task and consists of CA, National Intelligence Service and private experts etc.
- In order to discuss the following, the head of Certification Management Center should convene Certification Association, if necessary.
- Details about the certification policy for the operation of certification task
- Details about improvement of the system and maintenance of related laws for spread of GPKI use
- Details about mutual connection between Certification Authorities and international cooperation
- Details required to ensure safety and reliability and promote the use of GPKI

1.3.6 National Computing and Information Service

National Computing and Information Service is a national authority operating the main information and communication infrastructure of government authorities.

All of GPKI certification system are transferred to the assets of National Computing and Information Service and are operated in accordance with the operating procedures of the national main information and communication infrastructure. With respect to the certification management work, it supervises physical security for the certification system, access control to the system and approval work.

1.3.7 Korea Local Information Research and Development Institute

Korea Local Information Research and Development Institute is an authority left in charge of the operation of Certification Management Center from the Minister of Government Administration and Home Affairs.

It performs the operational work to maintain GPKI certification system.

1.4 Certificate usage

1.4.1 Certificate type and usage

A certificate for certification authorities issued by Root CA is used to issue a certificate for registration authorities, individuals and authorities.

1.4.2 Limitation of GPKI usage

GPKI certificate should be used according to the issued purpose and use and prohibited from being used out of the scope and purpose of use.
Also, you should not use an expired or cancelled certificate.

1.5 GPKI CPS administration

1.5.1 GPKI CPS establish and revision

Certification Management Center establishes GPKI Certification Practice Statement and administers revision for maintaining the consistency of the certification policy.

1.5.2 Contact of GPKI CPS

The contact information of persons in charge related to GPKI Certification Practice Statement is as follows:

URL: www.gpki.go.kr
E-mail: gpki@korea.kr

1.5.3 Responsibility of GPKI CPS

The head of Certification Management Center is responsible for the establishment and revision of GPKI Certification Practice Statement.

1.5.4 Revision of GPKI CPS

In the case of technical or procedural changes, it should obtain the approval of the head of Certification Management Center to revise GPKI Certification Practice Statement.

1.6 Definitions and acronyms

- GPKI certificate (GPKI): The electronic information issued for confirm • prove the authenticity of GPKI to responsible person who in charge of the task in corporation• institution and group or the authority which conformed to Article 2 Paragraph 9 of Electronic Government Act.
- GPKI private key: Refers to electronic information used to generate GPKI.
- GPKI public key: Electronic information used to verify GPKI and refers to the information which is contained in the certificate.
- GPKI: Refers to legally effective electronic signature used by administrative agencies and officials.

- Hash Function: A function which is mapping any length of the character string to the fixed length of the binary character string

  It produces results with methods of cutting and substituting data or changing the position and these results are called a hash value. A hash function is one of important functions applied in integrity, certification, and non-repudiation of data.

- Electronic signature: Information to check the identity of a person who created the electronic document and the change status of electronic document. Refers to characteristic of the electronic document.

- Certification task: Means the task of management certificate and records related to certification, such as certificate issuance• renewal • revocation, subscriber information registration• change, notice of certificate• Certificate Revocation List (CRL), etc.

- Certificate Revocation List (CRL): List of certificates which lost certificate validity, and means electronic information periodically issued by CA.

- Certification Authority (CA): Is a trusted authority issuing an electronic signature certificate. It issues a CRL periodically and in charge of Certification task such as publication of certificate and CRL in the directory system

- Certification: The action that checking and proving the GPKI key is only key belonging to the subscriber.

- Online Certificate Status Protocol (OCSP): Means Online Certificate Status Verification Protocol to verify the certificate status in real time without obtaining CRL

- Registration Authority (RA): Means a certification authority that performing Certification task such as checking the identity of a subscriber, registering• managing subscriber information, certificate application and certificate revocation application.

- Object Identifier (OID): GPKI certificate includes the basic information such as subscriber (DN), issuer, version etc., in additionally includes algorithm, certificate policy, key usage, certificate properties. The target expressed by information is called an object. By the method assigning a unique number to each object is used to identify these objects without overlapping, it is called as OID.

- Subscriber: Means an individual or corporation · institution and organization receiving a certificate issued by a CA

- TSA(Time Stamp Authority): The authority checking and notifying a specific time the electronic document is presented to the CA, only in requested electronic document.

- LDAP (Lightweight Directory Access Protocol): Is a directory system access protocol used in the communication between directory server and client. It means a protocol made more concisely and practically than DAP
- DN (Distinguished Name): Means a unique name given to clearly distinguish subscriber objects. Standardized identification name contained in GPKI certificate to identify if administrative agencies, officials have a unique certificate.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Certification Management Center should publish GPKI Certification Practice Statement (CPS) on the homepage of Certification Management Center (www.gpki.go.kr).

Certification Management Center should publish a certificate and the status information of the certificate in the government directory system (ldap://cen.dir.go.kr). When there is change on certification, Certification Management Center must modify and publish it.

If necessary, Certification Management Center should modify published GPKI Certification Practice Statement (CPS).

If Certification Practice Statement (CPS) is changed, the Center should manage the revised version and effective date.

2.1 Repositories

Certification Management Center should publish an application form and related rules required for GPKI certification service including GPKI Certification Practice Statement on the homepage of Certification Management Center.

Certification Authority Revocation List (ARL) and information of issued certificate should be published in the government directory system.

2.2 Publication of certification information

Homepage: www.gpki.go.kr

E-mail: gpki@korea.kr

2.3 Frequency of publication

If GPKI Certification Practice Statement and the application form of GPKI certificate are changed, publish them on the homepage of Certification Management Center. Publish Certification Authority Revocation List (ARL) once a week.

2.4 Access controls

Anyone be able to access to the Information published on the homepage of Certification Management Center.

2.5 Maintenance of accurate information

Certification Management Center should accurately maintain the information of CPS and Certification Authority Revocation List.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming (name of certificate and DN system)

Name of GPKI certificate and DN system should comply with X.509 rules.

3.1.1 Types of names (DN)

Certificate DN name issued by a CA should comply with cn name, ou name ,o=,c=kr system.

CA certificate cn : cn=certification authority separator (2)+authority code (7)+ Serial Number (2)

3.1.2 Certification Issuance for Anonymity of subscribers

Not applicable

3.1.3 Uniqueness of names(DN)

DN of GPKI certificate would be a unique value.

3.1.4 Rules for interpreting various name forms

Names for GPKI basic area and interpretation rules are must contain meaningful identification system under GPKI technical requirements 3.OID and DN system.

3.1.5 Using GPKI trademarks

Not applicable

3.2 Initial identity validation

3.2.1 CA Initial Identity Validation

Root CA should issue a CA certificate only to Certification Authorities (CA) notified by the Minister of Government Administration and Home Affairs.

CA certificate should be issued after checking the public key of CSR file.

3.2.2 Organization Initial Identify Validation

(CA) If the administrative standard code of an authority that created GPKI certification application (for authority) is verified, CA will be recognized as a trusted authority.

3.2.3 Individual Initial Identify Validation

Not applicable

(CA) If personnel information is registered in the government directory system, CA should trust the identity of individual.

3.2.4 Issuance Certification for Non-verified Subscriber

Root Ca must not issue a certificate for the certificate applied by non-verified subscriber.

3.2.5 Validation of authority

The authority of a certificate is in effect as soon as the certificate issued.

CA should confirm that the domain's owner is certificate applicant based on the information queried from qualified registrant or the government-run database.

3.2.6 Criteria for interoperation

Root CA is interoperated with National Public Key Infrastructure system (NPKI) based on Certificate Trust List (CTL).

3.3 Identification and authentication for re-key requests

Not applicable

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

CA must apply in official document to issue CA certificate.

Certification Authority Public Key which is in form of PKCS#10 Certificate Signing Request (CSR) should attached when send official document.

4.1.1 Who can submit a certificate application

In accordance with Article 89 Paragraph 1 of the implementing ordinances of Electronic Government Act, only an authority left in charge of Certification task by the Minister of Government Administration and Home Affairs can apply for CA certificate.

4.1.2 Enrollment process and responsibilities

The CA should submit accurate application information and be responsible for the application information.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Root CA must check the accuracy of the information and identification applied by a CA only through official documents.

Generally, it checks identification by official documents applied by name of the department head of the authority or head of an organization. The certification information is disclosed to the applicant who went through the identification process.

4.2.2 Approval or rejection of certificate applications

In process of verify official document and applicator identity, Root CA must reject issue certificate in following circumstances:

- Falsity of application
- Applicant is considered not eligible to represent CA
- Applicant is considered as not qualified to manage CA work and technical work

The approval and rejection of the application should be replied in official documents.

4.2.3 Time to process certificate applications

Certification Management Center should issue a certificate within 30 days.

4.3 Certificate issuance

In accordance with Article 30 of the implementing ordinances of Electronic Government Act (certificate issuance), a certificate issued by Certification Management Center should include the following:

- Name of the administrative agency to be certified
- GPKI public key of a joining authority etc.
- Method of GPKI used by a joining authority and the CA
- Serial number of certificate
- Effective period of certificate
- Name of the competent CA
- If limiting the use range or purpose of the certificate, details about this
- If joining authorities have a confrontation with each other, details about this

4.3.1 CA actions during certificate issuance

When issuing a certificate, Certification Management Center should check the following:

- Derive GPKI public key and DN from the request form (CSR) submitted by the application authority
- Check the uniqueness of GPKI public key
- Check if GPKI public key is consistent with GPKI private key possessed by the CA
- Check the uniqueness of DN and specification compliance

4.3.2 Notification Issuance of Certificate

Certification Management Center should notify in the official document, As soon as issuing a CA certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

A CA should accept a CA certificate by official document and cannot reject unless there is a special reason.

4.4.2 Publication of the certificate by the CA

Certification Management Center should publish the certificate in the public repository (directory), as soon as issuing a CA certificate.

4.4.3 Notification of certificate issuance by the CA to other entities

Certification Management Center should publish the fact that a certificate has been issued on the web. If necessary, notify it to relate other entities.

4.5 Key pair and certificate usage

4.5.1 GPKI private key and certificate usage

GPKI private key only used as performing Certification task such as electronic signature and encryption communication etc.

4.5.2 GPKI public key and certificate usage

Certification Management Center should use GPKI public key only for the purpose stated in the extension field.

- It is set when used to verify the signature of the certificate. This bit corresponds only to Certification Authority certificate (KeyCertSign)
- It should be set when used to verify the signature of Certificate Trust List (CTL), Certificate Authority Revocation List (ARL), and Certificate Revocation List (CRL). In the case of Certification Management Center, this bit corresponds only to Certification Authority certificate (CRLSign).

A certification authority provides CRL to the issued certificate. Generally, a CA certificate should be published in the public repository (directory) and is used when verifying X.509 based path.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

A CA certificate can be renewed within the effective period of Root CA certificate.

4.6.2 Who may request renewal

Only the authority left in charge of Certification task by the Minister of Government Administration and Home Affairs can request renewal of a CA certificate.

4.6.3 Processing certificate renewal requests

It is the same with issuance process and certificate must not be renewed except for 4.6.1.

When renewing a certificate, Certification Management Center should check the following:

- Derive GPKI public key and DN from the request form (CSR) submitted by the application authority
- Check the uniqueness of GPKI public key
- Check if GPKI public key is consistent with GPKI private key possessed by the CA

- Check if DN is the same as DN issued in the past and specifications are observed

4.6.4 Notification of renewal certificate to subscriber

After renewing a CA certificate, Certification Management Center should notify it by official document.

4.6.5 Conduct constituting acceptance of a renewal certificate

Approve the certificate renewal in accordance with 4.6.3 of this document. Reply approval or rejection by official document.

4.6.6 Publication of the renewal certificate by the CA

Certification Management Center should publish the certificate in the public repository (directory) as soon as renewal the CA certificate.

4.6.7 Notification of certificate issuance by the CA to other entities

Certification Management Center should publish the fact that a certificate has been renewed on the web. If necessary, notify it to relate other entities.

4.7 Certificate re-issuance

In the event of a disaster such as GPKI private key damage of a CA, CA certificate must be revoked the certification, and do not reissuing the certification.

4.8 Certificate modification

In the case of changing the name of CA, CA certificate unnecessary to modify.

In the case of standard was modified, CA certificate should be issued newly.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Certification Management Center must revoke the CA certificate as following reason:

- If Certification task is not performed any longer such as organization dissolution of the CA
- If GPKI private key of the CA was damaged
- If the CA applied for certificate revocation
- If the CA did not apply the Certification task within 2 years from the date of being left in charge of Certification task

4.9.2 Who can request revocation

Only the authority left in charge of certification task by the Minister of Government Administration and Home Affairs can apply for revocation of a CA certificate. Root CA can revoke a CA certificate based on 4.9.1.

4.9.3 Procedure for revocation request

Revoke a certificate based on 4.9.1.

4.9.4 Publication of the revocation

When revoking a CA certificate, Certification Management Center should renew Certification Authority Revocation List (ARL). If necessary, notify it to relevant certification authorities,.

4.9.5 Time Within Which Root CA Must Process The Revocation Request

A CA certificate revocation should be processed within 30 days after receiving official documents.

After revoking CA certificate, the information must be included in next Certification Authority Revocation List (ARL), and it should be stored in the public repository (directory).

4.9.6 Revocation checking requirement for relying parties

A certificate verifier should check the certificate validity by ARL.

4.9.7 ARL issuance frequency

Root CA shall update are reissue Certification Authority Revocation List (ARL) at least once every seven days.

4.9.8 Maximum latency for ARL

Certification Authority Revocation List (ARL) issuance is periodically operated automatically.

4.9.9 On-line revocation/status checking availability

Not applicable

4.9.10 On-line revocation checking requirements

Not applicable

4.9.11 Other forms of revocation advertisements available

Not applicable

4.9.12 Special requirements re-key or key damage

When CA GPKI private key is damaged, the CA should report it to the Root CA immediately; send an official document for CA certificate revocation application according to key damage. The Root CA must revoke the CA certificate.

4.9.13 Circumstances for suspension

Not applicable

4.10 Certificate status services

Not supported

4.11 End of Certificate Service

The head of a CA with the reasons for cancellation of certification task such as reorganization, etc. should transfer the certification task of the competent authority to the CA designated by the Minister of Government Administration and Home Affairs in consultation with Certification Management Center. The services of the certification task of a CA are terminated by the change notification of the Minister of Government Administration and Home Affairs.

4.12 Key escrow and recovery

Not applicable

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

GPKI certification system is located in the main information and communication infrastructure designated by the country, and it is operated in accordance with the national management regulations.

5.1.2 Physical access

GPKI certification system allows only the entry and access of outsiders approved by the control of security personnel and the access history is recorded.

5.1.3 Power and air conditioning

In preparation for the risk of power outages and transformation, GPKI certification system receives power from Uninterruptible Power Supply (UPS).

The computer room where GPKI certification system is located should maintain the proper temperature and humidity.

5.1.4 Water exposures

To be protected safely from flooding, GPKI certification system should be installed away from the computer room floor.

5.1.5 Fire prevention and protection

GPKI certification system should be operated in space where fire detection and automatic fire extinguishing equipment are installed.

5.1.6 Media storage

Make a backup by using the backup equipment in order to protect the key information from the risk of loss and damage of data stored in the GPKI certification system.

5.1.7 Waste disposal

When disposing of the GPKI certification system, National Computing and Information Service should handle it safely depending on the type of waste.

5.1.8 Off-site backup

In order to protect the data of GPKI certification system, it is backed up remotely in the backup center separated physically.

5.2 Procedural controls

5.2.1 Trusted roles

In order to ensure the trust of GPKI certification system, the operating officer of Certification Management Center should specify and approve trusted roles.

Specified trusted roles should be current every year.

5.2.2 Number of persons required per task

- The certification task policy manager should establish, register, maintain and revise GPKI certification task policy.
- The security manager should secure, control and manage Certification Management Center such as access control etc.
- The certification task operation manager should handle all of task related to installation and operation of certification system and operating maintenance work.
- The certification system operator should perform certification system operation and maintenance tasks by placing two or more employees.
- Service Desk should perform counseling services for customer inquiries.
- A person in charge of key generation should perform CA key generation and activation work.
- The certification task developer should manage certification homepage etc.

5.2.3 Identification and authentication for each role

The work manager of Certification Management Center should control the access to Certification Management Center through the identity card and fingerprint.

When accessing certification task system, he/she should control the access with each individual certificate.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Operating personnel should acquire nationally recognized information and communication related qualification or have equivalent work experience.

5.3.2 Background check procedures

Operating personnel of GPKI certification system should have no reasons for disqualification in the result of national identification.

5.3.3 Training requirements

Certification task performing person should complete security regulations, internal management procedures and technical training required to perform the task.

5.3.4 Retraining frequency and requirements

Certification task performing personnel should complete security and related technical training every year.

5.3.5 Job rotation frequency and sequence

Not applicable

5.3.6 Sanctions for unauthorized actions

Take disciplinary action for personnel who did unauthorized actions in accordance with the relevant regulations and laws.

5.3.7 Independent contractor requirements

Not applicable

5.3.8 Documentation supplied to personnel

Personnel performing certification task can view the internal data required for work.

5.4 Audit logging procedures

For periodic audit, GPKI certification system should keep Log for major events.

5.4.1 Types of log

The application program (Root CA) should record the following event log.

- Event No.
- Date and time of the event
- Event information
- Event processing results

5.4.2 Frequency of processing log

Log should be reviewed once a week by the log auditor.

5.4.3 Retention period for audit log

By considering the availability and efficiency of management of storage space, the retention period of log should be 10 years depending on the type.

5.4.4 Protection of audit log

The deletion of audit log should be performed only by the authorized manager.

5.4.5 Audit log backup procedures

The log is backed up in real time.

5.4.6 Audit collection system

Log is stored in the internal system.

5.4.7 Notification to event-causing subject

The audit is not separately notified about auditing to individuals and authorities who causing log.

5.4.8 Vulnerability assessments

Vulnerability identifies the elements that are a threat to maintaining the function of the certification system and assesses the technical and managerial elements for reducing the possibilities.

5.5 Records archival

5.5.1 Types of records archived

Information which is required to issue GPKI certificate should be managed in records.

5.5.2 Retention period for archive

Retention period for archive should be 10 years.

5.5.3 Protection of archive

To prevent alteration, GPKI certificate application records should be converted to electronic files and stored in the information system. In order to protect the information from the loss of records, the information system should be backed up and managed regularly.

5.5.4 Archive backup procedures

The electronic records should be stored in a separate media by using the backup equipment.

5.5.5 Requirements for time-stamping of records

Not applicable

5.5.6 Archive collection system

Related records should be collected in the electronic payment system.

5.5.7 Procedures to obtain and verify archive information

After prior consultation with Certification Management Center, information related to GPKI certification system should be requested through the official document in the name of the requesting authority. Certification Management Center should reply in the official document for the request that received by official document.

5.6 Key changeover

In the case of the key effective period of GPKI certification system is expired or forgetting password of signature key, key compromise, GPKI certification system should re-issue a key with the same function and authority. The re-issuance procedures of a key should be carried out in the same procedure as the new key issuance procedures.

5.7 Compromise and disaster recovery

In the event of a disaster, GPKI certification system can continue work in a physically independent position and independent place.

5.7.1 Disaster recovery procedure of information system

In the case of a disaster causing serious risk to the work of GPKI certification system, restore the infrastructure and computing equipment in accordance with the disaster recovery procedures and continue the certification task in accordance with the disaster recovery procedures of GPKI certification center.

5.7.2 Information system resources are corrupted

Recover the certification system by using backed up key in accordance with the disaster recovery procedures.

5.7.3 Recovery procedure of key loss

In the case of compromise of CA signature key or occur risk of use, Certification Management Center should re-issue CA signature key and re-issue all keys issued to authorities and individuals.

5.7.4 Ensure Business continuity

GPKI certification system is operated as the main center and backup center system in accordance with national continuity plan. In the case of that the main center does not provide certification services due to a disaster, the backup center activates the

alternate operating system including infrastructure, information system and human resources.

5.8 CA or RA termination

As Root CA, Certification Management Center should notify the delegation termination of a CA and re-issue a certificate issued by the CA.

As a CA, Certification Management Center should notify the delegation termination of RA and prevent business gap during the delegation termination of RA.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation and installation

Root CA key pair should be generated in accordance with key generation procedures.

For key generation, use HSM which is certified as FIPS 140-2 Level 3.

Key generation task is carried out by the participation of at least authorized two members.

6.1.2 Private key delivery process

Not applicable

6.1.3 Public key delivery process

Root CA should submit CSR file in PKCS#10 formats as an attachment of official document to Certification Management Center.

6.1.4 Root CA public key delivery to relying parties

Publish Root CA certificate and fingerprint information on the website of Certification Management Center.

6.1.5 Key sizes

In order to use safe and reliable GPKI algorithm, use the key with the following size

- In the case of RSA, more than 2048 bits
- In the case of ECDSA, more than 224 bits

6.1.6 Public key parameters generation and quality checking

When issuing a new Root CA certificate, check if GPKI public key is consistent with GPKI private key owned by Root CA and check the uniqueness of DN and specification compliance.

6.1.7 Key usage purposes

Root CA key pair only used for usage specified in the X.509 extension field.

Usage is defined in 4.5.2 of this document

6.2 Private Key Protection and Cryptographic Module

6.2.1 Cryptographic module standards

Use a security module that meets 'Regulations regarding CA facilities and equipment' and FIPS-140-2 level 3.

6.2.2 Multi-person control

The multiple control of GPKI key management policy must be carried out by a person who contains access authority and multiple controls are performed under the participation of more than 2 people among appointed 3 people.

6.2.3 Private key escrow

Not applicable

6.2.4 Private key backup

The backup key of Root CA GPKI private key should be saved in Hardware Electronic Signature Module (HSM) backup equipment.

6.2.5 Private key archival

Root CA GPKI generating key(private key) backup equipment must be stored in a separate safe place.

6.2.6 Extraction of Private key

Not applicable

6.2.7 Private key storage on cryptographic module

It is stored safely inside of Hardware Electronic Signature Module (HSM).

6.2.8 Enabling private key

Root CA GPKI private key is enabled by using the operation key and password of multiple operators.

6.2.9 Disabling private key

The module is always enabled.

6.2.10 Method of destroying private key

If the Root CA key is no longer needed, it should be deleted from HSM partition. It also includes removal of a backup set.

6.2.11 Cryptographic Module Rating

See section 6.2.1 of this CPS.

6.3 Other aspects of key pair management

6.3.1 Public key archival

A public key is stored during the period of section 5.5.2 of this CPS.

A public key is included in Root CA system database.

6.3.2 Certificate operational periods and key pair usage periods

The period of Root CA certificate (Root) is 20 years and that of CA certificate is 10 years. The certificate is available up to the effective period.

6.4 Activation data

Activation data is the information required to operate and use Hardware Electronic Signature Module (HSM). Examples of the activation data include pin, cryptogram and key split system etc.

6.4.1 Activation data generation and installation

Activation data is generated in accordance with the specifications of Hardware Electronic Signature Module (HSM). This hardware is certified FIPS 140-2.

6.4.2 Activation data protection

The procedures used to protect activation data depend on pin number and key for access certification. Access certification Key is maintained by a designated manager.

A pin number is applied to the encryption policy of Certification Management Center.

6.4.3 Other aspects of activation data

Not specified.

6.5 Computer security controls

For the related system, comply with technical, managerial and physical security measures, and perform security checks activities for safe management.

6.5.1 Specific computer security technical requirements

The Root CA certification system has the access control function, identify and check operator function, audit log collection function and CTL/ARL generating function.

The certification system (CA) has the access control function, operator identification and check function, audit log collection function and CRL generating function.

6.5.2 System Security Technical Requirement

To access Root CA System, require more then 2 kind of security such as password, certificate, etc. The system access media are protected in a separate place.

6.6 Life cycle technical controls

6.6.1 System development controls

When changing or improving the function of Root CA certification system, controls are carried out under the approval of consignment authority, organizing authority.

6.6.2 Security management controls

There must be in proper segregation of duties among the computers that access Root CA system, at same time, minimize the access authority.

To access Root CA system, it needs approval of Certificate Management Center, RA, Organizing Authority, also change access authority periodically in the case of access person work change.

6.6.3 Life cycle security controls

Not applicable

6.7 Network security controls

The network is protected by intrusion detection system and intrusion prevention system

6.8 Time-stamping

NTP is used as time of Root CA certification system.

7. CERTIFICATE PROFILES

GPKI certificate and Certification Authority Revocation List (ARL) comply with "GPKI technical requirements."

7.1 Certificate profile Standard

Certification Management Center should comply with technical specifications of administrative electronic signature certification system. At same time, issue and notify GPKI certificate which is follow X.509 V3 standard.

7.1.1 Version number(s)

Certification Management Center should issue X.509 V3 certificate (The version field value is designated as number 2)

7.1.2 Certificate extensions

A certificate issued by Certification Management Center should use a certificate extension field stated in "GPKI technical requirements."

7.1.3 Algorithm object identifiers

Certificate algorithm OID should comply with "GPKI technical requirements" system.

sha256WithRSA Encryption	iso(1) member-body(2) us(48) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)
sha256	joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nisAlgorithm(4) hashAlgs(2) sha256(1)

7.1.4 Name forms

Issuer DN and subject DN should comply with "GPKI technical requirements" system.

7.1.5 Name forms

Not applicable

7.1.6 Certificate policy object identifier

The policy identifier (OID) of Certificate Policies should comply with "GPKI technical requirements" system.

7.1.7 Usage of Policy Constraints extension

The constraints of certificate policy field should comply with "GPKI technical requirements" system.

7.1.8 Policy qualifiers syntax and semantics

Not applicable

7.1.9 Processing semantics for the critical Certificate Policies Extension

Policy Qualifier Id within certificate extension field should comply with "GPKI technical requirements" system.

7.2 CRL profile Standard

When the organizational information of the certificate owner was changed or trust of the secret key was compromised, it is necessary to revoke the certificate.

X.509 V2 CRL is used in these technology requirements.

7.2.1 Version number(s)

CRL is used as X.509 V2 (The version field value is designated as number 1)

7.2.2 Extensions Field of CRL

The extension field of CRL should comply with "GPKI technical requirements" system.

7.3 OCSP profile Standard

Not applicable

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

All of GPKI Certification Practice Statement should comply with domestic and international legal systems and related technology standards and regular audits should be performed by an independent third party.

8.1 Frequency or circumstances of assessment

An audit should not exceed a maximum of one year, and be performed on a periodic basis.

8.2 Identity/qualifications of assessor

An audit should be performed by personnel with certain qualifications and skills as follows:

1. A person independent from the audited subject
2. A person with enough knowledge on domestic and international legal systems and related technology standards
3. Experts in PKI technology, information communication technology and information system audit
4. A person with related International qualification Web trust, ETSI or equivalent qualification

8.3 Assessor's relationship to assessed entity

An assessor should be free from in terms of finance or business with audited subject.

8.4 Topics covered by assessment

The scope of assessment should include the compliance status of GPKI Certification Practice Statement, CA key management, certificate management and Root CA (Root CA) system management.

8.5 Actions taken as a result of deficiency

Deficiencies and remarks found through assessment should be included in the report, policy and technical actions should be taken according to the assessment results, and the scope is determined depending on the effect.

8.6 Communication of results

The assessment results should be reported to the head of Certification Management Center.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

GPKI certification system is information protection based infrastructure operated by the country and does not charge the cost of issuance, re-issuance, renewal of a certificate and other fees to individuals or authorities.

9.2 Financial responsibility

There is any monetary compensation for the problems related to certification issued by GPKI certification system.

9.3 Confidentiality of classified information

GPKI certification center should safely protect the acquired and generated information related to certification services.

9.3.1 Scope of confidential information

Information that may reduce the safety and reliability of GPKI certification services should be managed as confidential.

9.3.2 Information not within the scope of confidential information

Information not affecting the safety and reliability of GPKI certification services should be disclosed.

9.3.3 Responsibility to protect confidential information

Confidential information of GPKI certification services should be kept safe and managed by the authorized personnel.

9.4 Privacy of personal information

GPKI certification center should safely manage personal information obtained by the certificate application in accordance with Privacy Act.

9.5 Intellectual property rights

All intellectual rights arising from GPKI certification system belong to the Ministry of Government Administration and Home Affairs.

9.6 Representations and warranties

9.6.1 CA representations and warranties

GPKI certification system complies with domestic relevant laws, statutes, enforcement regulation and rules

GPKI certification system complies with GPKI Certification Practice Statement (CPS) in CA task

In order to provide safe and reliable certification system, GPKI certification system complies with related standard and rules.

9.6.2 RA representations and warranties

Root CA is not applicable with respect to RA guarantee.

A CA should comply with GPKI Certification Practice Statement (CPS) with respect to RA task.

9.6.3 Subscriber representations and warranties

In order to use GPKI certification services, a user should provide accurate information.

A CA ensures the signature key algorithm and validation that can be trusted by users.

9.7 Disclaimers of warranties

Not applicable

9.8 Limitations of liability

Not applicable

9.9 Indemnities

Not applicable

9.10 Term and termination

Not applicable

9.11 Individual notices and communications with participants

Not applicable

9.12 Amendments

9.12.1 Procedure for amendment

In the case of GPKI Certification Practice Statement (CPS) need to change, it should obtain the approval of the head of GPKI Certification Center. In the case of minor changes or error corrections and the change is independent from the policy of GPKI Certification Practice Statement (CPS), modification can be made without prior approval.

9.12.2 Notification for amendment

In the case of a change in CPS, it should be published on the homepage of Certification Center (www.gpki.go.kr)

9.12.3 Circumstances under which OID must be changed

Not applicable

9.13 Dispute resolution provisions

Disputes arising in relation to GPKI certification system should follow the decision of the Minister of Government Administration and Home Affairs.

9.14 Governing law

GPKI Certification Practice Statement (CPS) should comply with the relevant law of the country and follow the higher law in the case of a conflict.

9.15 Compliance with applicable law

GPKI Certification Practice Statement (CPS) should comply with Electronic Government Act and applicable law.

9.16 Miscellaneous provisions

Not applicable

9.17 Other provisions

Not applicable