GPKI

CA(Certificate Authority)

Certificate Practice Statements

(CA CPS)

2017. 11.

< Contents >

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(Certification Practice Statement framework).

GPKI Certification Practice Statement is posted on the website of GPKI Government Certification Management Authority ('hereinafter Government Certification Management Authority'). Institutions or individuals using GPKI personal and institutional certificates can view the GPKI Certification Practice Statement at any time. This regulation is effective from the date of publication.

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 Types of GPKI certificate

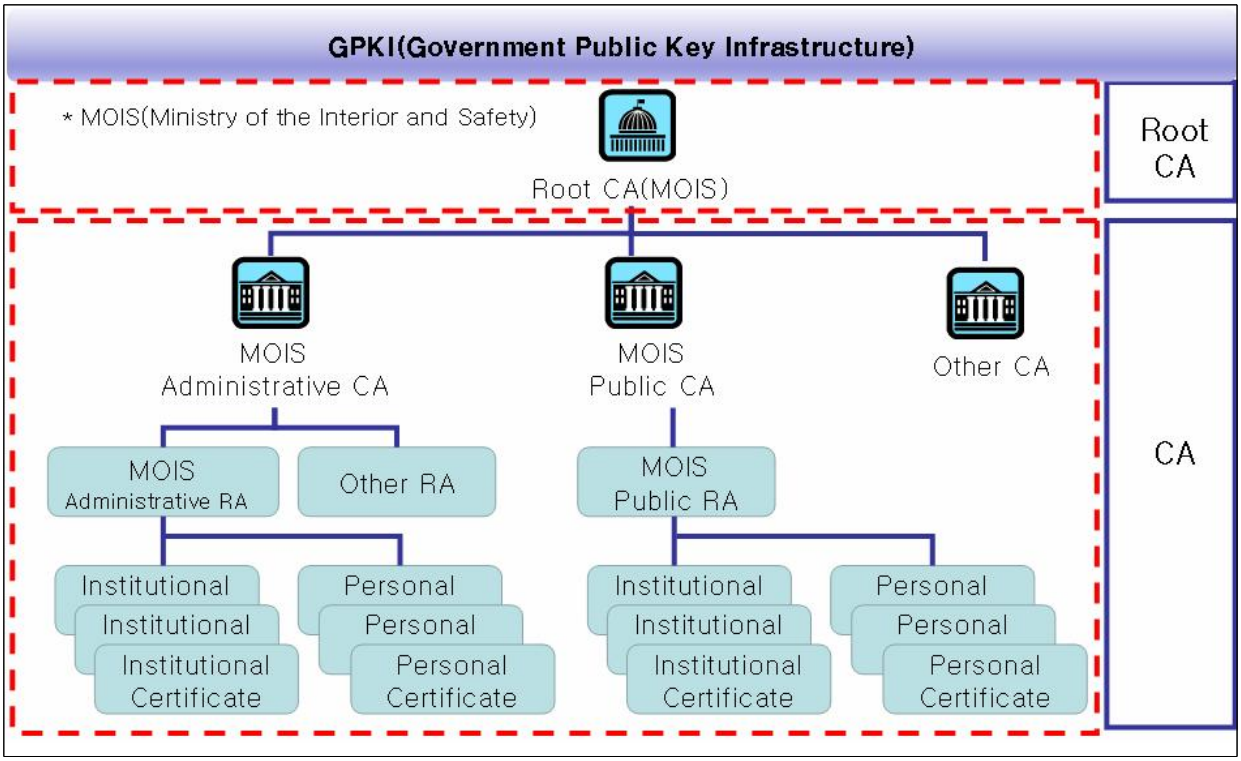
Types of GPKI certificate are issued by GPKI CA as follows

- For Administrative Agencies
  - Personal Certificate(1.2.410.100001.2.2.1)
  - Institutional Certificate(1.2.410.100001.2.1.1)
  - Computer(G-SSL) Certificate(1.2.410.100001.2.1.2)
  - Special-Purpose Certificate(1.2.410.100001.2.1.3)

- For Public Agencies
  - Personal Certificate(1.2.410.100001.2.2.2)
  - Institutional Certificate(1.2.410.100001.2.1.4)
  - Computer(G-SSL) Certificate(1.2.410.100001.2.1.5)
  - Special-Purpose Certificate(1.2.410.100001.2.1.6)

- Web service(G-SSL) Certificate(Government network only)
  - Web service(G-SSL) Certificate(1.2.410.100001.2.1.2)

1.3 GPKI certificate system



1.3.1 Ministry of the Interior and Safety

As a policy supervisory agency for safe and reliable operation of GPKI certification management system, the Ministry of the Interior and Safety 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
- Checking for the certification task operation status to ensure the safety and reliability of certification task

1.3.2 Government Certification Management Authority

Government Certification Management Authority is an agency of performing the work of Root CA and CA of GPKI certification system.

Government Certification Management Authority performs the following tasks.

- Designation of CA and certification task such as CA certificate

issuance and management etc.

- Establishment of CA facilities and equipment standards
- Checking 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 list created by Government Certification Management Authority
- Maintaining information and records related to CA management etc.
- Certification task related education for administrative/public agencies and subscribers belonging to GPKI certification management system
- Managing GPKI Technology Standards and providing interconnection plan between GPKI and authorized electronic signature
- Other tasks related to certification task as a Root CA
- Convocation and progress of Certification Council

1.3.3 Certificate Authority

GPKI CA(Certificate Authority) is designated authority by notification from the Minister of Ministry of the Interior and Safety.

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 keeping and management of records on certification task
- Other tasks such as time stamping service etc as a CA.

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's 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

Administrative · public CA can perform the independent RA tasks.

1.3.5 Certification Council

Certification Council is a consultative body composed to effectively perform certification tasks and consists of CA, National Intelligence Service and private experts etc.

In order to discuss the following, the head of Government Certification Management Authority should convene Certification Council, if necessary.

- Details about the certification policy for the operation of certification tasks

- Details about improvement of the system and maintenance of related laws for spread of GPKI use

- Details about interconnection between Certification Authorities and international cooperation

- Details required to ensure safety and reliability and promote the use of GPKI

1.3.6 National Information Resources Service

National Information Resources Service is a national agency operating the main information and communication infrastructure of government

agencies.
All GPKI certification systems are transferred to the assets of National Information Resources Service and operated in accordance with the operating procedures of the national main information and communication infrastructure. With respect to the certification management works, 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 agency left in charge of the operation of Government Certification Management Authority from the Ministry of the Interior and Safety.
It performs the operational work to maintain GPKI certification system.

1.3.8 Certificate subscriber

As public officials(or corresponding personnel) or administrative · public agencies that has been issued a certificate from Government Certification Management Authority, the subject of issuance is as specified in the CPS 4.1.1.

1.4 Certificate usage

1.4.1 Certificate types and usage

GPKI Certificates are issued for the following purposes depending on the subject of the issuance.
The certificate for the RA issued by the CA is used for the encrypted communication with the CA.
The personal certificate issued by the CA is used for administrative tasks such as user authentication and electronic approval.
The certificate for agencies issued by the CA is a certificate for the representative of the relevant organization and it issues only one certificate to the administrative, auxiliary, assistant organization etc.

The G-SSL certificate issued by the CA is used to support data encryption in the internet section between webpage and user computer.

The certificate for the servers issued by the CA is used for the telecommunication equipment of administrative and public agencies.

1.4.2 Limitation of GPKI certificate usage

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

1.5 GPKI CPS Management

1.5.1 GPKI CPS establish and revision

Government Certification Management Authority establishes GPKI Certification Practice Statement and it manages revision for maintaining the consistency of the certification policy.

1.5.2 Contact Information of GPKI CPS

The contact information 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 Government Certification Management Authority 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 Government Certification Management Authority to revise GPKI Certification Practice Statement.

1.6 Definitions and abbreviation

- **GPKI certificate (GPKI)**: The electronic information issued for confirm/prove the authenticity of GPKI to responsible person who in charge of the task in administrative/public agencies 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 digital signature**: 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 the 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. It 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)**: Trusted authority issuing an electronic signature certificate. It issues a CRL periodically and in charge of certification tasks such as publication of certificate and CRL in the directory system.
- **Certification**: The action that checking and proving the GPKI key belonging to the subscriber.
- **Online Certificate Status Protocol (OCSP)**: It means Online Certificate Status Verification Protocol to verify the certificate status in real time without obtaining CRL.

- **Registration Authority (RA)**: It 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. Each object is assigned unique number to identify these objects without overlapping, it is called as OID.
- **Subscriber**: Individual or Administrative/Public agencies and organization receiving a certificate issued by a CA
- **TSA(Time Stamp Authority)**: The authority checking and notifying a specific time from the electronic document is presented to the CA, only in requested electronic document.
- **LDAP (Lightweight Directory Access Protocol)**: 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)**: 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

Government Certification Management Authority publishes GPKI Certification Practice Statement (CPS) on the website of Government Certification Management Authority (www.gpki.go.kr).
Government Certification Management Authority posts certificates and the status information of the certificate in the government directory system (ldap://cen.dir.go.kr). When there is change on certification, Government Certification Management Authority modifies and posts it.
If necessary, Government Certification Management Authority modifies published GPKI Certification Practice Statement (CPS).
If Certification Practice Statement is changed, Government Certification Management Authority manages the revised version and effective date.

2.1 Repositories

Government Certification Management Authority posts an application form and related rules required for GPKI certification service including GPKI Certification Practice Statement on the website of Government Certification Management Authority.
Certification Revocation List (CRL) and information of issued certificate is posted in the government directory system.

2.2 Publication of certification information

Homepage(website) : www.gpki.go.kr
E-mail address : gpki@korea.kr

2.3 Frequency of publication

If GPKI Certification Practice Statement and the application forms of GPKI certificate are changed, Government Certification Management Authority posts them on the website. Certification Revocation List (CRL) is posted once a week. Individual and Institutional certificates are posted at the time of issuance.

2.4 Access controls

Anyone can access to the Information posted on the website of Government Certification Management Authority.

2.5 Maintenance of accurate information

Government Certification Management Authority accurately maintains the information of CPS and Certification Revocation List(CRL).

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming (name of certificate and DN structure)

Name of GPKI certificate and DN structure 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 structure. Certificate DN name issued by a CA for the purpose of web service Certificate(G-SSL) should comply with cn name,ou name,o=,s=,l=,c=kr structure.

- Computer Certificate cn : cn=authority separator(3)+authority code(7)+Serial Number(3)
- Web service Certificate(G-SSL) cn : cn=domain name
- Personal Certificate cn : cn=authority separator(3)+name+Serial Number(3)
- RA Certificate cn : cn=RA separator(2)+authority code(7)+Serial Number(2)
- Special-Purpose Certificate cn : cn=Special-Purpose separator(3)+authority code(7)+Serial Number(3)
- OCSP Certificate cn : cn=OCSP separator(4)+authority code(7)+Serial Number(2)
- TSA Certificate cn : cn=TSA separator(3)+authority code(7)+Serial Number(3)

3.1.2 Meanings of names

The information contained in the common name(cn) attribute or Subject Alternative Name attribute should identify the individual, authority or domain.

3.1.3 Certification Issuance for Anonymity of subscribers

Not applicable

3.1.4 Rules of names

The name and interpretation rules used in the base domain of the GPKI certificate have a meaningful identification scheme according to the GPKI technical requirements of 3.OID and DN structure.

3.1.5 Uniqueness of names(DN)

DN of GPKI certificate should be a unique value.

3.1.6 Using GPKI Trade marks

Not applicable

3.2 Initial Confirmation of Identity

3.2.1 Initial Confirmation of Identity for CA

Root CA should issue a CA certificate only to Certification Authorities (CA) notified by the Minister of Public Administration and Security.
CA certificate should be issued after checking the public key of CSR file.

3.2.2 Initial Confirmation of Identity for the Organization

CA shall be recognized as a trustworthy authority when the administrative standard code of the authority that created the application for administrative digital signature certification (for the authority) is confirmed.
In case of the web service certificate (G-SSL), the institutional name, e-mail address and domain information of the subscriber listed in certificate application form are compared with the information confirmed by WHOIS, and the applicant's first Initial Confirmation of Identity for the Organization is conducted. If necessary, telephone verification of the domain owner inquired by WHOIS is conducted. When the certificate is issued by CSR, the CA compares the CSR information with the registered and performs final verification. The Certification Authority should refuse to issue a certificate if the web service certificate (G-SSL) application address consists of an IP address.

3.2.3 Initial Confirmation of Identity for Individual

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

If necessary, additional identity verification of an individual may be carried out through a telephone verification procedure to confirm whether application for certificate is made through a separate agent(agency).

3.2.4 Certificate issuance for Non-verified Subscriber

A certificate is not issued for an application for an unidentified certificate. In case of web service certificate (G-SSL) only for government dedicated network, verification of the application domain through the WHOIS can be omitted.

3.2.5 The Effectivation of the authority

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

3.2.6 Criteria for inter-operation

Root CA is inter-operated with National Public Key Infrastructure system (NPKI) based on Certificate Trust List (CTL). Web service certificates(G-SSL) do not make cross certification.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and validation for routine re-key

Subscribers may apply for re-issuance in the following cases, and the identity verification procedure for the certificate re-issuance is the same as the new issuance procedure.

- If the effective period of the certificate has elapsed
- If the password of certificate is lost
- If administrative digital signature key is damaged, leaked, or changed.
- If the information related to the certificate, such as the organization name and the name of the subscriber, has changed

3.3.2 Identification and validation for re-key after revocation

Not applicable

3.4 Identification and validation for re-key for revocation request

If the subscriber revokes the certificate through the website of Government Certification Management Authority, it can be revoked directly after confirming the identity through a valid certificate. The revoked certificate is not available. If needed to be re-used, it should be reissued in accordance with the application procedure in accordance with this Certification Practice Statement (CPS) 4.1.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

The RA and the subscriber accesses the website, receive the necessary information and form, fill in the application form, and applies the application to the CA or RA as an official document.

4.1.1 Certificate application criteria

In accordance with Article 2, Paragraph 9 of the Electronic Government Act, an organization or a person in charge of the following matters should apply the certificate application.

- Administrative agencies, subsidiary agencies, counseling agencies and public officials
- Employees who are directly responsible for administrative affairs, such as pre-emptive clerks, petition officers, etc. (excluding short-term part-time employees within 6 months)
- Public agencies and officials who distribute administrative documents and electronic documents using the system established by administrative agencies.
- Public agencies, private institutions, and personnel in charge of sharing of administrative information under Article 36 (2) of the Electronic government Act

4.1.2 Enrollment process and responsibilities

The RA and subscribers must be accurate in their certificate application information and be responsible for the content of the submission.

4.2 Certificate application processing

4.2.1 Performing identification and authentication

The CA can designate and manage the RA, and the RA can designate and manage the subordinate LRA(Local RA).

The CA and RA(LRA) can, in accordance with this Certification

Practice Statement (CPS) 3.2, confirm the accuracy and identity of the subscriber information with an official document. In general, the identity can be confirmed by an official document of the head of the relevant department or head of the agency. Certification information is provided only to the applicant who has undergone the identity verification process.

4.2.2 Approval or rejection of the certificate application

The CA should refuse the application if the application is found to be false or the applicant does not qualify as a representative of the authority during the identification process of the submitted document and the applicants. Approval and rejection of the application must be returned by an official document.

The RA(LRA) should refuse the application if it is impossible to verify the identity of the applicant based on the submitted document or the documents of applicant's has misrepresented in the application form or the submitted documents. The approval of the application provides an approval processing message, and the rejection of the application must be returned in an official document.

4.2.3 Time required to process the certificate application

The RA(LRA) issues a certificate within 30 days.

4.3 Certificate issuance

The certificate issued by Government Certification Management Authority must include the following items in accordance with Article 30 of the Electronic Government Act Enforcement Decree (issuance of certificates).

- Name of Applicant (Subject Name)
  - For personal use, name to distinguish between organization and individual
  - Name of organization in case of institutional(organizational) use
  - Name to distinguish between organization and server when it is for server use
  - The distinguished name of the domain for G-SSL

- Name to distinguish between authorities and tasks in case of special purpose use
- Name of CA and RA in case of organization performing certification work

- The GPKI digital signature verification key (public key)
- The GPKI signature method used by the applicant and the CA
- Certificate serial number
- Certificate validity period
- Name of the authorized CA
- The limit on the scope or use of certificates
- (OID) that can identify the issuer of the certificate.

4.3.1 CA actions during certificate issuance

Government Certification Management Authority confirms the following contents when issuing the certificate.

- Verify that the applicant is a member of the organization
- Whether the applicant's identity is confirmed
- Use valid reference number / authorization code
- (For G-SSL) Domain ownership
- (For G-SSL) Certificate Signing Request (CSR) in PKCS # 10 format File Integrity and Electronic Signature

4.3.2 Notification of certificate issuance

The RA certificate should be notified by Government Certification Management Authority after issuing the certificate.
The certificate for the subscriber is sent to the applicant as soon as the certificate is issued. The message provided to the subscriber may be SMS or E-MAIL.

4.4 Receiving the certificate

4.4.1 Procedure for receiving the certificate

The RA receives the certificate application as an official document and accepts the certificate registration unless there are special reasons. The certificate can be issued for 15 days after registering, and the

certificate issuance out of the time limits does not allowed for security issues.
The subscriber certificate is issued by the applicant himself through the website.

4.4.2 Publication of the certificate by the CA

Government Certification Management Authority posts the certificate to the public repository (government directory system) at the same time as issuing the Certificate Authority certificate. However, Web service certificate (G-SSL) is not posted separately.

4.4.3 Notification of Certificate issuance by the CA to other entities

Not Applicable

4.5 Key pair and certificate usage

4.5.1 GPKI private key and certificate usage

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

4.5.2 GPKI public key and certificate usage

The certificate issued by Government Certification Management Authority should only use for the purposes specified in the administrative digital signature verification key (public key) extension field.

- Digital Signature is used for such purposes as entity authentication, data origin authentication with integrity, and so on.
- Non-Reputation is set when it is used to verify digital signature to provide non-repudiation services.
- KeyEncipherment is set when used for key transport. For example, when the RSA key is used for key management.
- DataEncipherment is set when it is used to encrypt the owner's data.
- KeyAgreement is set when used for key agreement. For example, a Diffie-Hellman key is set when it is used for key management.

- EncipherOnly is used only for data encryption while the owner public key performs a key agreement when the keyAgreement bit is set.
- DecipherOnly is set when the owner public key is used only for data decryption while performing the key agreement (key agreement) when the keyAgreement bit is set.

The CA posts a valid subscriber certificate issued to a public repository (directory). In general, a public repository (directory) can be utilized in case of obtaining the public key of the subscriber certificate.

4.6 Certificate renewal

4.6.1 Certificate renewal criteria

The certificate renewal is renewable within a valid certificate expiration date of 100 days.
Renewal of RA certificate is required to be renewed with an official document to the CA.
The renewal of the certificate for the subscriber can be directly renewed by the user using the website. However, web service certificate (G-SSL) is excluded.
The renewal of the web service certificate (G-SSL) can only be renewed through the website after approval of the renewal with an official document.

4.6.2 Certificate Renewal Applicants

Only the subject of this document 4.1.1 can apply for certificate renewal.

4.6.3 Procedure for Certificate renewal requests

It is the same as the new issuance procedure, certificate renewal should be allowed only for the case of document 4.6.1. A subscriber renewal certificate can only be renewed if it has a valid certificate issued.
Web service certificate (G-SSL) renewal can be renewed only after

newly created and submitted CSR in PKCS # 10 format in web server.

4.6.4 Notification of renewal certificate to subscriber

The RA certificate should be notified by Government Certification Management Authority after the certificate is renewed.
The certificate for the subscriber is sent to the applicant as soon as the certificate is renewed. The message provided to the subscriber may be SMS or E-MAIL.
Government Certification Management Authority should provide the user with a certificate renewal notice message 100 days before the effective certificate expiration date for the convenience of the subscriber.

4.6.5 Confirmation for Certificate renewal requests

No separate approval is required if you have an existing certificate that is valid in accordance with this document 4.6.3.
The web service certificate (G-SSL) must be approved by the administrator upon renewal. The approval of the application provides an approval processing message, and the rejection of the application must be returned in an official document.

4.6.6 Publication of Certificate renewal

Government Certification Management Authority posts the certificate to the public repository (government directory) at the same time the certificate is renewed. However, the web service certificate (G-SSL) is not posted separately.

4.6.7 Notification of Certificate renewal by the CA to other entities

Not Applicable

4.7 Certificate re-Issuance

4.7.1 Certificate re-Issuance criteria

Subscriber can apply for re-issuance of the certificate to the RA for the reasons listed below.

- The certificate has expired.
- If the applicant wants to obtain a certificate that is concerned that the administrative digital signature generation key (private key) has been exposed, lost or changed
- When certificate-related information is changed.

4.7.2 Certificate re-Issuance applicants

Only the subject of this document 4.1.1 can apply to re-issuance of the certificate.

4.7.3 Procedure for Certificate re-Issuance requests

Subscribers submit a certificate re-issuance application to the RA's representative with an official document.
The RA(LRA) officially confirms the identity of the submitted document and issues a re-issuance approval. A message is sent to the subscriber in the approval process.
The subscriber performs the certificate re-issuance procedure in the same manner as the new issuance procedure.

4.7.4 Notification of re-Issued certificate to subscriber

The RA certificate should be notified by an official document after the certificate is reissued from Government Certification Management Authority.
The certificate for the subscriber is sent to the subscriber as soon as the certificate is reissued by the RA(LRA) administrator and the subscriber re-issues the certificate.
The message provided to the subscriber may be SMS or E-MAIL.

4.7.5 Conduct constituting acceptance of a re-Issued certificate

The RA certificate is approved by the CA representative.
The certificate for the subscriber should be approved by the RA(LRA).

4.7.6 Publication of the Certificate re-Issuance

Government Certification Management Authority posts the certificate to

the public repository (government directory) at the same time that the RA certificate or subscriber certificate is reissued. However, the web service certificate (G-SSL) is not posted separately.

4.7.7 Notification of Certificate re-issuance by the CA to other entities

Not Applicable

4.8 Certificate modification

(For personal certificates) If the name of the subscriber or organization is changed, the certificate will be revoked immediately. The post-deletion process follows the new registration procedure.

4.8.1 Circumstances for certificate modification

If the information in the subscriber's certificate is changed, such as the name of the subscriber, the name of the authority(organization), the subscriber must change the certificate. To change the certificate, the certificate must be reissued after revoking the existing certificate.

4.8.2 Subject of certificate modification

The subject of the certificate change is the same as this Certification Practice Statement (CPS) 4.1.1. .

4.8.3 Certificate modification processing

Government Certification Management Authority, the RA and the LRA are required to comply with the validation process of this Certification Practice Statement (CPS) 3.2. and the certificate request is processed.

4.8.4 Notification of certificate issuance

Follows this Certification Practice Statement (CPS) 4.3.2. .

4.8.5 Procedure for Receiving the certificate

Follows this Certification Practice Statement (CPS) 4.4.1. .

4.8.6 Publication of the modified certificate by the CA

Government Certification Management Authority publishes the

certificate to the public repository (government directory) at the same time that the RA certificate or subscriber certificate is re-issued. However, the Web Service certificate (G-SSL) is not posted separately.

4.8.7 Notification of Certificate modification by the CA to other entities

Not Applicable

4.9 Certificate revocation and suspension

4.9.1 Certificate revocation criteria

The CA and the RA should revoke the certificate in the event of any of the following.

- The subscriber has applied for certificate revocation.
- The subscriber is aware of the fact that the certificate was issued in an illegal manner.
- If recognized that the information (name, organization information, etc.) in the subscriber's certificate has changed
- If the subscriber's GPKI digital signature generation key (private key) is recognized as being lost, damaged or stolen
- If the CA's digital signature generation key (private key) used in the subscriber's certificate is found to be lost, corrupted, stolen, leaked or unsafe
- Other, if it is deemed necessary to revoke the certificate
- In case of founding changes in the status of employment (retirement, transfer, etc.)

4.9.2 Certificate revocation applicants

Only the authority or the person in charge of this document 4.1.1, or the person entrusted with the certification work by the Minister of Public Administration and Security, can apply for the certificate revocation.

4.9.3 Procedure for Certificate revocation requests

In case of a subscriber certificate, if subscriber have a valid certificate,

subscriber can revoke it through the website directly.
If the subscriber lost his existing certificate, the subscriber can request the RA representative to revoke the certificate.
The RA(LRA) can process the certificate revocation request to the CA in case of resignation or reorganization.

4.9.4 Publication of the revocation

Government Certification Management Authority posts the certificate revocation list (CRL) in the public repository (government directory) everyday when the subscriber certificate is revoked. It also provides a real-time certificate status validation (OCSP) service. The revoked certificate is deleted from the public repository (government directory) immediately upon revocation.

4.9.5 Time required to process the certificate revocation request

RA(LRA) representative should process the request for revocation of the subscriber certificate within 30 days after receipt of an official document. The CA's work is handled automatically by connection systems when the certificate is revoked due to the retirement or reorganization of the RA(LRA) subscriber.
However, the revocation of the web service certificate (G-SSL) should be processed within 24 hours.

4.9.6 Revocation checking requirements for relying parties

The certificate verifier must verify the validity of the certificate using a certificate revocation list (CRL). The certificate revocation list (CRL) of a certificate is obtainable through the address specified in the CRL DP (distribution point) entry. A CRL DP (distribution point) can have a URL address of an authorized government directory (LDAP) or HTTP.

4.9.7 CRL issuance frequency

The certificate revocation list (CRL) is issued everyday.

4.9.8 Maximum lead time for CRL issuance

Issuance of Certificate Revocation Lists (CRLs) is periodically handled automatically.

4.9.9 On-line revocation/status check availability

The OCSP service validates the certificate based on the certificate's revoked time. The address of the OCSP service for each certificate is as follows.

- Administrative personal / organizational Certificate: http: //gva.gpki.go.kr:8000

- Public personal Certificates: http://ocsp.gpki.go.kr:8000

- Web service Certificate: http://ssl-ocsp-gov.gpki.go.kr:8100

4.9.10 On-line revocation checking requirements

The certificate verifier must validate the certificate using OCSP. The OCSP server accepts a GET Method HTTP request from the OCSP validation requestor.

4.9.11 Alternative ways for validating certificate revocation information

Government Certification Management Authority provides SCVP (Server Based Certification Validation Protocol) services in addition to CRL and OCSP.
The certificate verifier can verify the validity of the certificate using SCVP.

4.9.12 Special requirements re-key or key damage

The subscriber should apply for re-issue of the certificate according to the key impairment to the RA by an official document when the GPKI digital signature generation key (private key) of the subscriber is damaged. The RA(LRA) representative re-issue the certificate.
If the certificate of the RA is damaged in the digital signature

generation key (private key) of the RA, apply to the CA for a re-issuance of the RA's certificate by an official document. The certificate of the RA is reissued by CA and returned as an official document.

4.9.13 Circumstances for suspension

Not Applicable

4.9.14 Certificate suspension applicants

Not Applicable

4.9.15 Procedure for Certificate suspension requests

Not Applicable

4.9.16 Limits on suspension period

Not Applicable

4.10 Certificate status services

4.10.1 Functional feature

The certificate status can be checked with the certificate revocation list(CRL) and the real-time certificate status confirmation service(OCSP).

4.10.2 Service availability

The Certificate Status service is provided without a 24x365 interruption unless there is a planned interruption.

4.10.3 Optional features

Not Applicable

4.11 End of certificate service

The RA(LRA) where the reason for termination of the certification work occurred, such as reorganization, must taken over the certification work

of the relevant authority to the RA designated by the CA by consultation with the CA. The authentication service of the RA(LRA) terminates the service when all the subscriber's certificates are terminated.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

It provide a key escrow service capable of selectively storing a subscriber's private key.

4.12.2 Session key encapsulation and recovery policy and process

When the subscriber uses the key escrow service, the private key is divided and encrypted and stored in the three escrow servers. If the subscriber wishes to recover the key, the subscriber should perform the key recovery directly from the website of Government Certification Management Authority after confirming an official document.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and facility

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

5.1.2 Physical access

GPKI certification system should allow 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 the space where fire detection and automatic fire extinguishing equipment are installed.

5.1.6 Media storage

GPKI certification system should be made 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 Information Resources 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 manager in charge of Government Certification Management Authority should specify and approve trusted roles.
Specified trusted roles should be updated every year.

- The certification task policy manager should establish, register, maintain and revise GPKI certification task policy.
- The security manager should secure, control and manage Government Certification Management Authority such as access control etc.
- The certification task operation manager should handle all of the tasks 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 subscriber's inquiries.
- The person in charge of key generation should perform CA key generation and activation work.
- The certification task developer should manage certification website etc.
- The internal auditor performs periodic self-checks on the operation

of Government Certification Management Authority.

5.2.2 Manpower per major task

The policy manager and the key generation manager designate two or more people and perform their duties.

5.2.3 Identification and authentication for each role

The work manager of Government Certification Management Authority should control the access to Government Certification Management Authority through the identity card and fingerprint.
For the control of certification task system, the access should be performed by each individual certificate.

5.3 Manpower management

5.3.1 Qualification requirements

Operation staffs should acquire nationally recognized information and communication related qualification or have equivalent work experience.

5.3.2 Identification

Operation staffs of GPKI certification system should not have any reason for disqualification in the result of national identification.

5.3.3 Training requirements

Certification task performing staffs should complete security regulations, internal management procedures and technical training required to perform the task.
- Information security (laws, regulations, manuals, etc.) and personal information protection education
- Procedures for handling Government Certification Management Authority and roles, responsibilities, etc.
- PKI-based technology and latest certification trend education
- Training on identity verification procedures

5.3.4 Retraining requirements

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

5.3.5 Job rotation

Not Applicable

5.3.6 Sanctions for unauthorized actions

It should be took disciplinary actions 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 Disclosure of documents

Staffs performing certification tasks can view the internal data required for work.

5.4 Audit logging procedure

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

5.4.1 Types of audit Log

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

- Event No.
- Date and time of the event
- Event details
- Event processing results
- Certificate lifecycle-related logs
- CA Key lifecycle-related Logs
- The access log and request log for the CA system.

5.4.2 Frequency for audit log review

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 audit logs should be protected from tampering by unauthorized person such as retrieving, modification, deletion, etc.

5.4.5 Audit log backup

The log is backed up in real time.

5.4.6 Audit collection system

Logs are stored on the internal system.

5.4.7 Notification of log target

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

5.4.8 Vulnerability assessment

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

5.5 Records archival

5.5.1 Types of records archived

It records the information necessary for issuing GPKI digital signature certificates. Types of records include the audit logs specified in 5.4.1.

5.5.2 Retention period for archive(Records)

Retention period for archive(Records) should be 10 years.

5.5.3 Protection of archive(Records)

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(Records) 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 approval system.

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key changeover

In case the key effective period of GPKI certification system is expired or password loss 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 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 procedures for Information system

In case of a disaster causing serious risk to the work of GPKI

certification system, it should be restored the infrastructure and computing equipment and continued the certification task in accordance with the disaster recovery procedures of GPKI certification center.

5.7.2 Recovery procedures for damaged information system resources

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

5.7.3 Recovery procedures for key loss

In case of compromise of CA signature key or risk of use occurrence, Government Certification Management Authority should re-issue CA signature key and re-issue all keys issued to authorities and individuals. Periodic key recovery tests should be taken according to disaster recovery scenarios in preparation for key loss due to disasters.

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 case 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 of delegation

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

As a CA, Government Certification Management Authority 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

The CA key pair should be generated in accordance with key generation procedures.
For key generation, it uses HSM which is certified as FIPS 140-2 Level 3. Key generation task is carried out by the participation of at least two authorized members.
The subscriber's GPKI digital signature generation key (private key) pair is generated using the 'certificate management software' provided to the subscriber. Key generation uses HSM which is certified as FIPS 140-2 Level 3.

6.1.2 Private key delivery process

Provide CA's digital signature generation key (private key) - Not applicable
Delivery of Subscriber GPKI Digital Signature Generation Key (Private Key) - The software creates a secret key on behalf of the subscriber and delivers the GPKI digital signature generation key (private key) and certificate to the subscriber.

6.1.3 Public key delivery process

The CA submits the PKCS # 10 format CSR file to the CA as an attachment to the official document.
The subscriber's GPKI public key is transmitted to the CA after the corresponding software generates the subscriber's key pair.

6.1.4 CA public key delivery to relying parties

It posts the Certificate Authority (CA) certificate and fingerprint information on Government Certification Management Authority website.

6.1.5 Key sizes

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

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

6.1.6 Public key parameters generation and quality checking

It checks whether the new CA certificate and the digital signature verification key (public key) match with the GPKI digital signature generation key (private key) owned by the CA, and checks the uniqueness and compliance of the DN.
In case of issuing new subscriber certificate, it checks the integrity of CMP request using authorization code HMAC.

6.1.7 Key usage purposes

It is used only 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

It uses 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 controls of GPKI key management policy must be carried out by the people who have access authority and multiple controls are performed under the participation of 2 or more people among appointed 3 people.
The GPKI digital signature generation key (private key) of subscriber authority is securely transmitted through encrypted communication.

6.2.3 Private key escrow

The CA's GPKI digital signature generation key (private key) is not applicable.

The private key of the subscriber includes an GPKI digital signature generation key (private key) and a private key for distributing the encryption key. Among them, the private key for distribution for cryptography can be selectively entrusted and stored.

6.2.4 Private key backup

The backup key of CA's GPKI private key should be saved in Hardware Electronic Signature Module (HSM) backup equipment.
The subscriber's private key stored on the consignment server is backed up to the off-site storage.

6.2.5 Private key archival

The backup equipment of the CA's GPKI digital signature generation key (private key) must be stored in a separate safe place.
The subscriber's private key is divided into three, encrypted and stored. The private key stored on the entrusted server is persistent.

6.2.6 Extraction of Private key

The CA's GPKI digital signature generation key (private key) is encrypted and extracted from a hardware security module (HSM) for backup purposes.

6.2.7 Private key storage on cryptographic module

The CA's GPKI digital signature generation key (private key) is stored safely inside of Hardware Electronic Signature Module (HSM).

6.2.8 Enabling private key

The CA's GPKI digital signature generation key (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 deleting/destroying private key

If the CA key is no longer needed, it is deleted from the HSM

partition. It also includes the removal of backup sets.
The private key of the subscriber stored in the consignment server is not deleted.

6.2.11 Cryptographic Module Rating

It complies with the cryptographic module classes specified in 6.2.1 of the Certification Practice Statement (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 the CPS.
A public key is included in CA system database.

6.3.2 Certificate operational periods and key pair usage periods

The period of CA certificate is 10 years and that of subscriber certificate is 2 years 3 months. 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 Government Certification Management Authority.

6.4.3 Activation data transmission

Not specified.

6.5 Computer security controls

For the related system, it complies with technical, managerial and physical security measures, and perform security check activities for safe management.

6.5.1 Specific computer security technical requirements

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 CA System, it requires 2 or more kinds of security requirements 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 CA certification system, controls are carried out under the approval of consignment organization, managing organization.

6.6.2 Security management control

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

To access CA system, it needs approval of Government Certification Management Authority, consignment organization, managing organization, also change access authority periodically in case of access person's 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 CA certification system.

7. CERTIFICATE PROFILES

GPKI certificate, Certification Revocation List (CRL) and real-time Certificate Status Validation (OCSP) comply with "GPKI technical requirements."

7.1 Certificate profile Standard

Government Certification Management Authority should comply with technical specifications of public electronic signature certification system, issue and notify GPKI certificates which follow X.509 V3 standard.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

A certificate issued by Government Certification Management Authority 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(840) 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) nistAlgorithm(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 constraints

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

In case organizational information of the certificate owner is changed or reliability of the secret key was damaged, 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

Government Certification Management Authority should comply with the [Technical Specification for Real-time Status Verification of GPKI Digital Signature Certificate] in order to provide the reliability of GPKI digital signature certificate validation function when using of

authentication service in the GPKI digital signature authentication system.

7.3.1 Version number(s)

Real-time Certificate Status Verification (OCSP) is used with X.509 V1. (The version field value is specified as the number 0)

7.3.2 OCSP extensions

The extension field of OCSP complies with the "GPKI technical requirements" system.

8. AUDIT COMPLIANCE AND OTHER ASSESSMENTS

All matters 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 Webtrust, 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 Scope of assessment

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

8.5 Actions for assessment results

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 Declaration of assessment results

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

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(organizations).

9.1.1 Certificate issuance or renewal fees

No charge

9.1.2 Certificate access fees

No charge

9.1.3 Revocation or status information access fees

No charge

9.1.4 Fees for other services

No charge

9.1.5 Refund policy

Not Applicable

9.2 Financial responsibility

There is no monetary compensation for the problems related to certification issued by GPKI certification system.

9.2.1 Insurance coverage

Not Applicable

9.2.2 Other assets

Not Applicable

9.2.3 Insurance or warranty coverage for end-entities

Not Applicable

9.3 Confidentiality of classified information

Government Certification Management Authority 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 Personal information protection

GPKI Government Certification Management Authority should safely manage personal information obtained by the certificate application in accordance with the Personal Information Protection Act.

9.4.1 Privacy plan

Government Certification Management Authority should comply with related laws and regulations such as the Personal Information Protection Act. and collects, holds, and processes personal information in accordance with the personal information processing policy posted on the website.

9.4.2 Processed personal information

Collect and retain personal information in accordance with the personal information processing policy posted on the website.

9.4.3 Information not closed

Not Applicable

9.4.4 Responsibility for personal information protection

Government Certification Management Authority should comply with related laws and regulations such as the Personal Information Protection Act. and collects, holds, and processes personal information in accordance with the personal information processing policy posted on the website.

9.4.5 Notification and consent to personal information usage

Government Certification Management Authority should comply with relevant laws and regulations such as the Personal Information Protection Act. and notify the use of personal information and obtain consent of the information subject through the website and application forms.

9.4.6 Disclosure pursuant to judicial or administrative procedure

Not Applicable

9.4.7 Disclosure criteria for Other information

Not Applicable

9.5 Intellectual property rights

All intellectual rights arising from GPKI certification system belong to the Ministry of the Interior and Safety.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

9.6.1.1 Limited warranties

GPKI certification system should comply with domestic relevant laws, regulations, enforcement rules and rules. GPKI certification system should comply with GPKI Certification Practice Statement (CPS) in CA task. GPKI certification system should comply with related standard and rules in order to provide safe and reliable certification system.

9.6.1.2 Warranties and obligations under CA Browser Forum

Not Applicable

9.6.2 RA Representations and Warranties

Root CA is not applicable with respect to RA guarantee.
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. CA ensures the signature key algorithm and validation that can be trusted by users.

9.6.4 Relying Party Representations and Warranties

Not Applicable

9.6.5 Representations and Warranties of Other Participants

Not Applicable

9.7 Disclaimers of warranties

Not applicable

9.8 Limitations of liability

Not applicable

9.9 Exemption from liability

9.9.1 Indemnification by Subscribers

Not applicable

9.9.2 Indemnification by Relying Parties

Not applicable

9.10 Term and termination

9.10.1 Term

Certificate practice statement are effective after posted to the repository (website).

9.10.2 Termination

Certificate practice statement and related policy documents remain in effect until they are revised to a new version.

9.11 Individual notices and communications with participants

Not applicable

9.12 Amendments

9.12.1 Procedure for amendment

In case of GPKI Certification Practice Statement (CPS) need to change, it should obtain the approval of the head of GPKI Government Certification Management Authority. In 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 case of a change in CPS, it should be posted on the website of Government Certification Management Authority. (www.gpki.go.kr)

9.12.3 Changes of OID

Not Applicable

9.13 Dispute resolution provisions

Disputes arising in relation to GPKI certification system should follow the decision of the Ministry of the Interior and Safety.

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

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Separation clause

Not applicable

9.16.4 Enforcement(Abandonment of attorney's fees and rights)

Not applicable

9.16.5 Irresistible force

Not applicable

9.17 Other provisions

Not applicable