# GSSL
# Certification Practices Statement(CPS)

2024. 3.

Ministry of the Interior and Safety

# Revision History

| Version | Date | Revision Description | Prepared by | Approved by |
|---|---|---|---|---|
| 1.0 | ‘23.2.9 | Creates first revision of certification practice statement(CPS) in accordance with RFC 3647 and CA/Browser Forum standards | Euiyeol Choi | Changyun Han |
| 1.1 | ‘23.4.14 | Details revised in accordance with RFC 3647 and CA/Browser Forum standards | Euiyeol Choi | Changyun Han |
| 1.2 | ‘24.2.6 | Changed OCSP certificate validation period | Dongwha Shin | Changyun Han |
| 1.3 | ‘24.3.29 | Reflecting the latest CA Browser Forum TLS BRs:<br>- modified Section 9.4.6, Certificate Profile and others<br>- updates to fixing terms and spelling errors | Dongwha Shin | Changyun Han |
|  |  |  |  |  |

# <Table of Contents>

# 1. INTRODUCTION

## 1.1. Overview

The MOIS SSL certificate infrastructure has been established as a PKI system dedicated to issuing TLS Certificates (hereinafter "GSSL Certificate" in abbreviation of "Government SSL Certificate") by the Ministry of the Interior and Safety(hereinafter "the MOIS") in the pursuit of providing the integrity and confidentiality into e-government and public electronic services. This document defines certification policy and operational management procedures employed in certification authority services provided by the MOIS.

This document is structured in accordance with the Internet Engineering Task Force (IETF) standard RFC 3647, and the Certificate Authority issuing GSSL Certificate conforms to the current version of "CA/Browser Forum(CABF) Baseline Requirement for the Issuance and Management of Publicly-Trusted Certificates" published by CA/Browser Forum at http://www.cabforum.org.

## 1.2. DOCUMENT NAME AND IDENTIFICATION

This document is Certification Practice Statement (CPS) which describes the policies on the operation and management of the GSSL Root Certification Authority(hereinafter "GSSL Root CA") and GSSL Certification Authority (hereinafter "GSSL Sub CA" and, together with Root CA, "GSSL CA"). In detail, it specifies the legal, and technical requirements of certification services to relying parties and Subscribers, which include approval, issuance, renewal, re-key, management, use, validation, and revocation of Certificates.

## 1.3. PKI PARTICIPANTS

### 1.3.1. Certification Authorities

The Root CA performs the following tasks:

- Validation of certificate authorities
- Revision of Certification Practice Statement (CPS), Terms of Use, and Privacy Policy
- Issuance, renewal, revocation of certificates and publication of Authority Revocation List(ARL)
- Validation of Certificate issued by root certification authority
- Safe storage and management of records related to certification tasks
- Inspection of CA operations to ensure safety and reliability of certification tasks

The CA performs the following tasks:

- Issuance, renewal, revocation of subscriber certificates and publication of Certification Revocation List(CRL)
- Validation of certificates issued by the CA
- Safe storage and management of records related to certification tasks
- Inspection of CA operations to ensure safety and reliability of certification tasks

### 1.3.2. Registration Authorities

The Registration Authority (RA) refers to entities that approve and perform requests to issue, renew, reissue, and revoke subscriber certificates. The GSSL CA, as the RA, identify and authenticate applicant representatives and/or applicants requesting certificates and validate the submitted application information, and does not operate any external RA.

### 1.3.3. Subscribers

Subscribers are authorized governmental/public organization to use Subscriber Certificates issued by the GSSL CA, and Subscribers have Subscriber Certificates. According to section 3.2 and in order to use the

Certificate, he/she must agree to the responsibilities and obligations described in the Terms of Use prior to issuing the Certificate.

### 1.3.4. Relying Parties

A relying party is an entity that verifies a digital signature with a certificate issued by GSSL CA or decrypts an encrypted document or a message.

### 1.3.5. Other Participants

#### 1.3.5.1. The Ministry of the Interior and Safety (The MOIS)

The MOIS is the policy supervisory Ministry for the safe and reliable operation of the GSSL CA and is charged with the following.

- Establishment and operation of the GSSL CA
- Due diligence and Request corrective actions on the GSSL CA
- Amendments of CPS

#### 1.3.5.2. National Information Resources Service

The National Information Resources Service(hereinafter the “NIRS“) is a national agency that operates Critical Information Infrastructure of Korean government agencies.

The GSSL CA systems are delegated to NIRS and managed, and operated in accordance with the National Mission-Critical IT infrastructure operational procedures of NIRS. In regard to certification service management duties, the NIRS takes charge of physical security for the certification system, access control and approval for the system.

#### 1.3.5.3. Korea Local Information Research & Development Institute

The Korea Local Information Research & Development Institute (hereinafter the “KLID”) is the authorized public entity entrusted with the operation of the GSSL Root CA and GSSL CA by the Minister of the

MOIS.

The GSSL Center is the dedicated organization which belongs to KLID to directly operate the GSSL CA.

The GSSL Center(hereinafter the "Center" ) performs the following.

- Issuance and management of CA Certificates
- Establishment of standards for facilities and equipment of CA
- Inspection of the safe operation of facilities and equipment of the CA or managerial activities corresponding thereto
- Publish CA Certificate and CRL of CA
- Archive all Certificates and CRL generated within GSSL CA.
- Maintaining information and records related to the management of CA.
- Training related to certification tasks for all personnel included in the GSSL chain of operations
- Other duties deemed necessary in connection with or to certification duties

## 1.4. CERTIFICATE USAGE

### 1.4.1. Appropriate Certificate Uses and Types

Certificates issued in accordance with this CPS are used for the purposes of Server Authentication and Client Authentication as defined in the Extended Key Usage field. The GSSL CA issues OV certificates.

### 1.4.2. Prohibited Certificate Uses

Certificates are prohibited from the uses that are inconsistent with the scope and purpose for which it was issued. In addition, the use of terminated or revoked Certificates is prohibited. The certificate does not ensure the reliability, compliance, and safety of transaction, and only proves that the information in the certificate has been accurately validated at the time of certificate issuance. Subscriber Certificates uses are restricted to the encryption of the information exchange between end-entity browsers and the Subscriber's website which has been validated in accordance with section 3.2, section 4.2.

## 1.5. POLICY ADMINISTRATION

### 1.5.1. Organization Administering the Document

The MOIS establishes the CPS and amends the CPS at least once a year to maintain its consistency with the latest requirements of the CA/Browser Forum.

### 1.5.2. Contact Person

Contact details of the CPS are the following:

- Tel: +82 1661-9088(Ext. 2)
- Fax: +82 02)2031-9363
- URL: ssl.gpki.go.kr
- Email: gssl@klid.or.kr
- Address: 301, Seongam-ro, Mapo-gu, Seoul, Republic of Korea (03923)

### 1.5.3. Person Determining CPS Suitability for the Policy

The MOIS minister is responsible for establishment and amendment of the CPS. The amendment records in document history of the CPS include the version of the CPS, reason for change, etc.

### 1.5.4. CPS Approval Procedures

The GSSL CA shall revise the CPS with the approval of the MOIS upon technical or procedural changes. Any changes are disclosed at the location described in section 2. In case of a possibility of a significant impact on the subscriber due to the amendment, the subscriber may be notified.

## 1.6. DEFINITIONS AND ACRONYMS

### 1.6.1. Definitions

- Applicant : Refers to a institution, or organization that has applied for a certificate to obtain a GSSL Certificate.
- Applicant Representative : Refers to an personnel representing an Applicant for the issuance of a GSSL Certificate.
- CA/Browser Forum : Refers to a voluntary group of certificate authorities (CAs), vendors of internet browser software, and suppliers of other applications that use X.509 digital certificates for TLS and

code signing.

- Certification : Refers to the action that validates the GSSL Certificate key being the only key belonging to the Subscriber.
- Certification Authority(CA) : Refers to a trusted authority that issues digital signature Certificates, periodically issues a Certificate Revocation List(CRL), and is responsible for certification tasks such as posting the Certificate Authority(CA) Certificate and Certificate Revocation List(CRL) on the website.
- Certificate Revocation List(CRL) : Refers to a list of Certificates that lost Certificate validity, and means electronic information periodically issued by Certification Authority(CA).
- Certification tasks : Refers to the task of managing Certificates and records related to certification, such as Certificate issuance, renewal, revocation, Subscriber information registration, change, a notice of the Certificate, Certificate Revocation List(CRL), etc.
- Certificate Transparency: Refers to an Internet security standard that allows all certificates to be recorded and identified in the public log system to monitor and audit the issuance of Certificates.
- Cryptographically Secure Pseudo-Random Number Generator(CSPRNG) : A random number generator intended for use in cryptographic system.
- Distinguished Name(DN) : Refers to a unique name given to clearly distinguish a subscriber object.
- GSSL Certificate: Refers to electronic information issued to corporations, authorities, and organizations which belongs to the 9 of Article 2 of the Electronic Government Act and is used for encryption and decryption to safely protect information transmitted between electronic government websites and user browsers.
- GSSL Certificate Generation Key(Private Key) : Refers to electronic information held by subscribers and used to generate a GSSL Certificate.
- GSSL Certificate Validation Key(Public Key) : Refers to electronic information included in the Certificate and used to validate the GSSL Certificate.

- Hash function : Refers to a function that 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 hash values. A hash function is one of the important functions applied in the integrity, certification, and non-repudiation of data.
- Internet Corporation for Assigned Name and Numbers(ICANN) : Refers to the organization established in 1998, composed of Internet business, technical, academic, and user organizations. It plays a role in coordinating tasks such as IP address space allocation, protocol parameter specification, and root server system management.
- National Intelligence Service : The Chief Management/Control Authority in national Cyber Security in South Korean governmental/public information systems.
- Object Identifier(OID) : Refers to the basic information of GSSL Certificates such as Subscriber(DN), issuer, version, etc., additionally includes algorithm, Certificate policy, key usage, and Certificate properties. The target expressed by information is called an object. The method of assigning a unique number to each object is used to identify these objects without overlapping, it is called OID.
- Online Certificate Status Protocol(OCSP) : Refers to the protocol that is used to verify the Certificate status in real time without obtaining Certificate Revocation List(CRL).
- Subject : Refers to the unique name of the owner written in the certificate.
- Subscriber : Refers to an organization or a group receiving a Certificate issued by a Certification Authority(CA).
- OV certificate: TLS certificate issued through verification of both identity and domain ownership of the applicant, and the verified information is displayed on the certificate so that can confirm the ownership of the site.

### 1.6.2. Acronyms

- ARL: Authority Revocation List
- CA: Certificate Authority or Certification Authority
- CAA: Certification Authority Authorization
- CABF: CA/Browser Forum
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- CSR: Certificate Signing Request
- CT: Certificate Transparency
- DN: Distinguished Name
- DNS: Domain Name System or Domain Name Service
- FIPS: (US Government) Federal Information Processing Standard
- FQDN: Fully Qualified Domain Name
- HSM: Hardware Security Module
- HTTP: Hypertext Transfer Protocol
- ICANN: Internet Corporation for Assigned Names and Numbers
- IETF: Internet Engineering Task Force
- NIS: National Intelligence Service
- NTP: Network Time Protocol
- OCSP: Online Certificate Status Protocol
- OID: Object Identifier
- OV: Organization Validation
- PKCS: Public Key Cryptography Standard
- PKI: Public Key Infrastructure
- PKIX: IETF Working Group on Public Key Infrastructure
- RA: Registration Authority
- RFC: Request for Comments (IETF.org)
- SCT: Signed Certificate Timestamp
- SHA: Secure Hashing Algorithm
- SSL: Secure Sockets Layer
- TLS: Transport Layer Security
- URL: Uniform Resource Locator
- UTC: Coordinated Universal Time

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The GSSL CA publishes Korean version/English Version of the CPS on the website(ssl.gpki.go.kr). The GSSL CA records and keeps the document history according to section 5.4.

## 2.1. REPOSITORIES

The GSSL CA makes the following information accessible via the online repository including GSSL CA CPS.

- GSSL CA CPS
- Most recently issued certificate revocation list(CRL)
- Most recently issued CA certificate revocation list(ARL)
- Root CAs and CA certificates issued by GSSL CA
- Other documents or information deemed necessary for the disclosure

The GSSL CA publishes the amended CPS in the online repository within seven (7) days after the CPS amendment.

## 2.2. PUBLICATION OF CERTIFICATION INFORMATION

The GSSL CA makes the Certificate issuance and management information accessible via the website for everyone with ease.

- Website: ssl.gpki.go.kr
- Email: gssl@klid.or.kr
- By Mail address to :301, Seongam-ro, Mapo-gu, Seoul, Republic of Korea (03923)
- Tel: +82 1661-9088(Ext. 2)
- Fax: +82 02)2031-9363

## 2.3. TIME OR FREQUENCY OF PUBLICATION

The CRL of the Subscriber Certificate is updated daily basis, and the CA CRL(ARL) of the CA certificate is updated at least every 364 days. The GSSL CA shall amend the CPS at least once a year in accordance with the latest CA/Browser Forum(CABF) Baseline Requirement.

## 2.4. ACCESS CONTROLS ON REPOSITORIES

The Repository is publicly available in a read-only manner. Logical and physical controls are implemented to prevent unauthorized modification or deletion of repository entries.

# 3. IDENTIFICATION AND AUTHENTICATION

## 3.1. NAMING

The Certificate naming and Distinguished Name(hereinafter the “DN” ) conform with ITU X.509 standard.

### 3.1.1. Types of Names

Subscriber OV Certificate’s DN contains the following attributes.

- CN=Common Name
- O=Organization Name
- L=Locality Name
- S=State or Province
- C=Country Code

### 3.1.2. Need for Names to be Meaningful

The GSSL CA puts meaningful names in both the subject DN and the issuer DN of Certificates which identify the subject and issuer respectively.

### 3.1.3. Anonymity or Pseudonymity of Subscribers

The GSSL CA does not issue anonymous or pseudonymous Certificates.

### 3.1.4. Rules for Interpreting Various Name Forms

The name forms used in basic field of Certificates are interpreted using X.500 standards and ASN.1 syntax.

### 3.1.5. Uniqueness of Names

The DN of the Certificate contains the domain name, and the uniqueness of the domain name is managed by the International Internet Address

Management Organization(hereinafter the “ICANN” ). The Fully Qualified Domain Name (FQDN) specified in the Subject Alternative Name is validated in accordance with section 3.2.2.4, and the serial number of the GSSL Certificate is unique and not reused.

### 3.1.6. Recognition, Authentication, and Role of Trademarks

No stipulation.

## 3.2. INITIAL IDENTITY VALIDATION

### 3.2.1. Method to Prove Possession of Private Key

The GSSL Root CA issues CA Certificate only to the GSSL Sub CA officially notified by the Minister of the MOIS. The CA Certificate is issued after confirming the public key of the CSR file.

A certificate applicant shall prove ownership of the Private Key by providing GSSL CA with a CSR in PKCS#10 format or a cryptographically equivalent proof.

### 3.2.2. Authentication of Organization and domain identity

The GSSL CA identifies and validates the applicant and every personnel, entities and domains specified in a Certificate in the following circumstances:

- During the Certificate application
- During the Certificate reissuance application

The validation of an Applicant Representative is conducted to ensure the legitimate authority to request SSL certificate issuance upon the circumstances specified in this CPS. All subject information in a certificate shall conform to the requirements of this CPS and be validated in accordance with the procedures in this CPS in order to:

- Identify the applicant and applicant representative requesting a Certificate

- Confirm the name and existence of the applicant
- Confirm presence of the applicant at the physical location(address)
- Confirm the ownership of domain names to be included in the Certificate
- Confirm whether the applicant has the authority to request a Certificate

### 3.2.2.1. Identity

For OV Certificate application, the GSSL CA validates the identity and address of the Applicant using documentation provided by, or communication with, at least one of the following:

- A government agency in the jurisdiction of the Applicant’ s legal creation, existence, or recognition
- A third party database that is periodically updated and considered a Reliable Data Source
- A site visit by the CA

Generally, the Certificate application is submitted online. When an Applicant completes and submits an online form on the official website, the GSSL CA verifies :

- The identity of the applicant and applicant representative; and
- The address of the applicant

| Identity Validation Target | Identity Validation Methods |
|---|---|
| Applicant Representative | • Collect Applicant Representative information(name, contact information, employment status, qualification for certificate issuance) at submission and/or through the Certificate application process. |
| Applicant | • The Applicant submits demonstrative information to the GSSL CA (e.g., an English Certificate of Business Registration issued by Home-Tax website of the National Tax Service within three (3) months).<br>• Inquire and validate the information submitted by the Applicant by a reliable third-party database (e.g., validation on the Home-Tax website of the National Tax Service).<br>• Validate the Applicant information (name, employment, |

| | |
|---|---|
| | qualification, etc.) by calling the Applicant and Applicant representative phone number confirmed in a trusted third-party database (e.g., 114.co.kr, etc.).<br>Note: 114.co.kr is government licensed Phone Number Directory service |
| Address of the Applicant | The Subject field of an OV Certificate only contains validated geographic address information attributes.<br>The information submitted by the Applicant is validated by comparison with a trusted third-party database.<br>Regarding address notation, if an international standard or an official government standard exists, it shall be prioritized. The general criteria for the GSSL CA to determine the address in the subject field of the Certificate are as following:<br>• Country Name(C): Use of two-letter country code according to ISO 3166-1 Alpha-2<br>(If the Country Name field is present, the GSSL CA blocks the proxy server to prevent Certificate applications from IP addresses assigned to countries other than the country where the Applicant Representative is physically located.)<br>• State or Province(S): Use of unabbreviated, subdivision names of states or provinces according to ISO 3166-2<br>• Locality or City(L): Use of the official English name of the city or town<br>In particular, in the case that the address information validated in the Applicant/Applicant Representative identity validation procedure and written address in the application are the same, validation is considered complete. |

In special cases, the GSSL CA may validate the identity of the Applicant through site visit and/or face-to-face methods.

### 3.2.2.2. DBA/Tradename

No stipulation.

### 3.2.2.3. Verification of Country

See section 3.2.2.1.

#### 3.2.2.4. Validation of Domain Authorization or Control

| Validation Methods | Descriptions |
|---|---|
| Email, Fax, SMS, or Postal Mail to Domain Contact | Via Email, fax, SMS, or postal mail, confirming the applicant' s control over the Fully Qualified Domain Name(hereinafter the "FQDN" ) and then receiving a confirming response utilizing the Random Value.<br>Random values are generated by the GSSL CA and remain valid for up to 30 days after generation.<br>(See section 3.2.2.4.2 of CA/Browser Forum Baseline Requirement) |
| Email to Domain Contact | (i) Send an email to one or more email addresses created by using 'admin' , 'administrator' , 'webmaster' , 'hostmaster' , or 'postmaster' as the local part, followed by the at-sign ( "@" ), followed by an Authorization Domain Name. An email address consists of a local part, @, and an authenticated domain in that order.<br>(ii) The random value is included in emails.<br>(iii) The random value is used to validate a received response.<br>Random values are generated by the GSSL CA and remain valid for up to 30 days after generation.<br>(See section 3.2.2.4.4 of CA/Browser Forum Baseline Requirement) |

#### 3.2.2.5. Authentication for an IP Address

No stipulation.

#### 3.2.2.6. Wildcard Domain Validation

No stipulation.

#### 3.2.2.7. Data Source Accuracy

All data sources are verified for reliability, accuracy, and stability from counterfeiting before being used for identification and authentication purposes. Evaluation of the data source accuracy and reliability is conducted in accordance with section 3.2.2.7 of the CA/Browser Forum Baseline Requirements. The validity period of data source re-validation is as follows.

- Legal existence and identity of the Applicant - no longer than 397 days

#### 3.2.2.8. CAA Records

See section 4.2.4.

### 3.2.3. Authentication of Individual Identity

The GSSL CA does not issue Certificates to individuals.

### 3.2.4. Non-Verified Subscriber Information

A Certificate contains only validated information; optional subfields within the Subject field must contain the validated information or leave it empty.

### 3.2.5. Validation of Authority

The GSSL CA validates the authenticity of the request for a Certificate using Reliable Method of Communication. The GSSL CA uses the methods listed in section 3.2.2.1 as Reliable Method of Communication. The authority of applicant representatives to request Certificates on behalf of requesting organization is verified in accordance with section 3.2.2.1. The GSSL CA only accepts applications for Certificate issuance from applicants validated in Reliable Method of Communication.

### 3.2.6. Criteria for Interoperation or Certification

No stipulation.

## 3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

The GSSL CA does not provide Certificate re-key. Procedures for re-key requests are the same as for Initial Certificate applications in section 3.2.

### 3.3.1. Identification and Authentication for Routine Re-key

See Section 3.2.2.

### 3.3.2. Identification and Authentication for Re-key After Revocation

No stipulation.

## 3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

If the subscriber does not use the key pair or suspects that it has been compromised, he/she can request revocation of the certificate on the website of the GSSL CA after user authentication. If the key pair of the CA or the Subscriber is compromised or suspected of being compromised, the GSSL CA may revoke the relevant CA or Subscriber Certificate in accordance with this CPS section 4.9.1. The CA notifies the Subscriber of the Certificate revocation.

# 4. CERTIFICATE life cycle OPERATIONAL REQUIREMENTS

This section describes the Certificate application procedure, and requirements for Subscribers, and other Relying Parties related to the Certificate life cycle.

- Certificate Application
- Certificate Application Processing
- Certificate Issuance
- Certificate Acceptance
- Key Pair and Certificate Usage
- Certificate Reissuance
- Certificate Revocation and Suspension
- Certificate Status Service
- End of Subscription
- Key Escrow and Recovery

## 4.1. CERTIFICATE APPLICATION

### 4.1.1. Who Can Submit a Certificate Application

CA certificate issuance is requested through submission of the CA public key in the form of PKCS#10 CSR. The only organization authorized as GSSL CA operator by the Minister of the MOIS pursuant to Article 89 (1) of the Enforcement Decree of the Electronic Government Act can apply for a CA Certificate. A subscriber certificate application must be submitted in an online application form on the website of the CA.

An applicant is a governmental department or public organization stipulated

in Articles 2 (9) of the Electronic Government Act that applies for a certificate to obtain a GSSL Certificate.
An applicant representative is an employee or legitimate delegate of the Applicant, and mostly, an employee of an applicant and is required to be registered as AC(Administrative Contact) in WHOIS repository. An applicant representative must acknowledge and agree to Terms of Use when he/she signs up to the website of the CA.

- Certificate request must contain domain name to be included in Subject field of a Certificate. The GSSL CA verifies Certificate request information by comparison with a trusted third-party database.
- Certificates revoked due to suspected phishing or fraud, and/or application information rejected for issuance, are stored in the internal database, which can be used to screen suspicious issuance requests.

### 4.1.2. Enrollment Process and Responsibilities

Regarding CA certificate issuance, GSSL Root CA confirms that the application form and application procedure of the CA have completed, and the CA shall be responsible for the reliability of the application.

Regarding subscriber certificate issuance, the CA confirms that an applicant has completed application requirements below before issuing the Certificate.

- Submission of electronic certificate application form
- An agreement to Terms of Use
- Submission of the supporting documents specified in application form
- Generation of key pair and CSR using secure tool
- Submission of CSR containing the public key

## 4.2. CERTIFICATE APPLICATION PROCESSING

The GSSL CA validates the accuracy of the information provided by an applicant. An applicant presents the public key to CA online in the form of a PKCS#10 Certificate Signing Request (CSR).

### 4.2.1. Performing Identification and Authentication Functions

Identification and authentication of the information submitted by the Applicant are performed in accordance with the procedures specified in section 3.2.

### 4.2.2. Approval or Rejection of Certificate Applications

The GSSL CA approves the Certificate request when validation of the application information is completed. The GSSL CA rejects the Certificate request if the following apply:

- The application information is not validated
- The request does not comply with the CPS
- The Public key does not meet requirements set forth in sections 6.1.5, 6.1.6 of CA/Browser Forum Baseline Requirements
- The Private key is weak (such as Debian weak key)

### 4.2.3. Time to Process Certificate Applications

Unless it is specified in the contract, there is no stipulated time required to process the Certificate application, and if the application form and submission documents are validated properly, the GSSL CA issues the Certificate within about 30 days from applying for the Certificate.

### 4.2.4. Certificate Authority Authorization (CAA) Records

The GSSL CA reviews the CAA record for each dNSName in the subjectAltName extension field of the Certificate to be issued, following the procedure described in RFC 8659. The following Issuer Domain Names in CAA 'issue' or 'issuewild' records recognize that the GSSL CA can issue a Subscriber Certificate.

- ssl.gpki.go.kr

The GSSL CA documents potential issuance that was prevented by a CAA record in detail to provide feedback to the CA/Browser Forum.

## 4.3. CERTIFICATE ISSUANCE

Certificates issued by the GSSL CA shall include the following information in accordance with the latest CA/Browser Forum Baseline Requirements:

- Distinguished domain Names
- Certificate validation key (public key)
- A serial number of the Certificate - All Certificates must contain a serial number greater than zero, a number of no less than 64 bits of output from a CSPRNG.
- Certificate validity period – no longer than 397 days
- Contents concerning restrictions on the scope or purpose of use of a certificate

Before issuing a Subscriber Certificate, the CA obtains Subscriber Agreement or a Terms of Use according to section 9.6.3 of the CA/Browser Forum Baseline Requirements.

### 4.3.1. CA Actions during Certificate Issuance

Regarding Certificate Issuance by GSSL Root CA, it is required for an authorized CA Engineer to deliberately issue a direct command in order to perform the certificate signing operation.

Regarding Subscriber certificate, once the Identification and Authentication procedures are completed in accordance with this CPS, the Certificate is generated and the appropriate key usage extension field is added.

The GSSL CA performs conformance linting prior to signing a Certificate over the pre-certificate and the issued certificate. Nonconformity found in linting is logged and issuance is rejected.

In support of Certificate transparency, Subscriber Certificates submit Certificates to three (3) or more CT log operators to receive a Signed Certificate Timestamp(hereinafter "SCT" ) and include it in Certificate's extended field.

### 4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

The GSSL CA delivers within a reasonable time after issuing certificate. As for subscriber certificate, notification is sent to the applicant via email.

## 4.4. CERTIFICATE ACCEPTANCE

### 4.4.1. Conduct Constituting Certificate Acceptance

The CA Certificate shall be stored in a security medium and be received by the CA, and shall not be rejected unless there is a special reason.

The Subscriber Certificate is downloaded by the applicant himself/herself via the website of the CA.

### 4.4.2. Publication of the Certificate by the CA

The GSSL CA publishes the Root CA certificate and the CA certificates in the repository.

### 4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.5. KEY PAIR AND CERTIFICATE USAGE

### 4.5.1. Subscriber Private Key and Certificate Usage

The Private Key of the Certificate is used only for encryption of transmission information between the validated Subscriber's website and the access browser.

The GSSL CA shall require, as part of the Terms of Use, that the subscriber makes the commitments and warranties in Section 9.6.3, provision 2) and provision 4) in this CPS.

### 4.5.2. Relying Party Public Key and Certificate Usage

No stipulation.

## 4.6. CERTIFICATE RENEWAL

### 4.6.1. Circumstance for Certificate Renewal

Certificate renewal refers to issuing a new Certificate with an extended expiration date without changing the same key pair and Subject information. The CA Certificate may be renewed within the validity period of the Root CA Certificate, and the GSSL CA does not offer Subscriber Certificate renewal, and the Subscriber is required to generate a new Key Pair and request a new Certificate in accordance with section 4.1. Certificate reissuance is possible 30 days before the Certificate expiration date.

A Subscriber may apply for a Certificate reissuance to the GSSL CA for the following reasons, and the GSSL CA shall issue a new Certificate in accordance with section 4.1 after approving the reissuance of the Certificate requested by the Subscriber.

- In the case where the certificate has expired;
- In the case where it is suspected that the Certificate Private Key has been exposed, compromised, lost, or modified; or
- In the case where the Certificate-related information has changed

### 4.6.2. Who May Request Renewal

See section 4.1.1.

### 4.6.3. Processing Certificate Renewal Requests

See section 4.2.

### 4.6.4. Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

### 4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

See section 4.4.1.

### 4.6.6. Publication of the Renewal Certificate by the CA

See section 4.4.2.

### 4.6.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.7. CERTIFICATE RE-KEY

### 4.7.1. Circumstance for Certificate re-key

Certificate re-key means the issuance of a new Certificate with a new Public Key, but without changing the validity period or any other information in the Certificate.

The GSSL CA does not provide Certificate re-key, and treats certificate re-key requests as requests for the issuance of a new Certificate so that section 4.1 Certificate Application shall be applied.

The GSSL CA discards the CA Certificate in the event of a disaster including compromise of the CA Certificate Private Key, and issue a new CA Certificate according to application stated in the section 4.1.

### 4.7.2. Who May Request Certification of a New Public Key

See section 4.1.1.

### 4.7.3. Processing Certificate re-keying Requests

See section 4.2.

### 4.7.4. Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

### 4.7.5. Conduct Constituting Acceptance of a re-keyed Certificate

See section 4.4.1.

### 4.7.6. Publication of the Issued Certificate by the CA

See section 4.4.2.

### 4.7.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.8. CERTIFICATE MODIFICATION

### 4.8.1. Circumstances for Certificate Modification

The GSSL CA does not modify previously issued subscriber certificates. Any request for certificate modification will be treated as a request for the issuance of a new Certificate.

### 4.8.2. Who May Request Certificate Modification

See section 4.1.1.

### 4.8.3. Processing Certificate Modification Requests

See section 4.2.

### 4.8.4. Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

### 4.8.5. Conduct Constituting Acceptance of a Modified Certificate

See section 4.4.1.

### 4.8.6. Publication of the Modified Certificate by the CA

See section 4.4.2.

### 4.8.7. Notification of Certificate Modification by the CA to Other Entities

No stipulation.

## 4.9. CERTIFICATE REVOCATION AND SUSPENSION

The GSSL CA supports Certificate revocation but does not allow temporary suspension or recovery of Certificates. When a Certificate is revoked, corresponding certificate serial number is added to the CRL and marked revoked. Responses to requests for revocation of Certificates and inquiries are available 24x7.

### 4.9.1. Circumstances for Revocation

#### 4.9.1.1. Reasons for Revoking a Subscriber Certificate

The GSSL CA revokes the Subscriber Certificate within 24 hours in either of following circumstances:

- A Subscriber requests to revoke the Certificate to the CA in writing;
- The Subscriber notifies the GSSL CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The GSSL CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
- The GSSL CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.
- The GSSL CA is aware of a proven method that can easily compute the Subscriber's private key corresponding to the public key of the Certificate (e.g., refer to https://wiki.debian.org/SSLkeys for the Debian vulnerable key)

The GSSL CA revokes the Subscriber Certificate within five (5) days in either of following circumstances:

- The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
- The GSSL CA obtains evidence that the Certificate was misused;
- The GSSL CA is made aware that a Subscriber has violated one or more of its material obligations under the Terms of Use;
- The GSSL CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant' s right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

- The GSSL CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- The GSSL CA is made aware of a material change in the information contained in the Certificate;
- The GSSL CA is made aware that the Certificate was not issued in accordance with these Requirements or the GSSL CA’ s Certification Practice Statement;
- The GSSL CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
- The GSSL CA’ s right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the GSSL CA’ s Certification Practice Statement; or
- The GSSL CA is made aware of a demonstrated or proven method that exposes the Subscriber’ s Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

#### 4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

The GSSL CA revokes the CA Certificate within seven (7) days in either of following circumstances:

- The Subordinate CA requests revocation in writing;
- The GSSL Sub CA notifies the GSSL CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The GSSL CA obtains evidence that the Subordinate CA’ s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
- The GSSL CA obtains evidence that the Certificate was misused;

- The GSSL CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certification Practice Statement;
- The GSSL CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The GSSL CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The GSSL CA’ s or Subordinate CA’ s right to issue Certificates under these Requirements expires or is revoked or terminated, unless the GSSL CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
- Revocation is required by the GSSL CA’ s Certification Practice Statement.

### 4.9.2. Who Can Request Revocation

Only certification authorities delegated by the MOIS can request the revocation of the CA Certificate. Regarding Subscriber Certificate, revocation can be requested by subscriber according to section 4.1.1 via Contact Points listed at GSSL CA website.

### 4.9.3. Procedure for Revocation Request

The GSSL CA revokes of the CA Certificate in accordance with the procedures below when the revocation requirements meet the section 4.9.1.

1. Report immediately to related authorities including the MOIS and the National Intelligence Service(NIS), and send an official letter of revocation of the CA Certificate.
2. When the CA Certificate is revoked, the CA CRL(ARL) is updated and the relevant authority is notified if necessary.

Subscriber Certificate revocation is processed according to the following procedure.

1. GSSL CA logs the identity of the requester who has filed the revocation of Certificate and the reason of reqeuest according to

section 3.4. GSSL CA may include its own reasons in the log.

2. GSSL CA may request confirmation of certificate revocation from the requester, where applicable, via out-of-band communication (e.g. telephone, fax, e-mail etc.).
3. If request is confirmed as originated from GSSL Sub CA or the Subscriber, the Certificate is revoked immediately.
4. For requests from third parties, GSSL CA investigates request and, if a revocation is warranted, revokes the Certificate within 24 hours of receipt.
5. If GSSL CA determines that revocation is appropriate, GSSL CA revokes the Certificate and update the CRL.

GSSL CA maintains capabilities to receive Certificate revocation requests and Certificate Problem Reports 24x7.

### 4.9.4. Revocation Request Grace Period

Subscribers are required to immediately suspend usage of Certificate Generation Key(Private Key) and Certificate and request revocation to GSSL Center under the following cases:

1. When the Certificate Generation Key(Private Key) is considered to be lost, damaged, stolen or leaked
2. Inaccurate or incomplete information of the Certificate
3. Expiration or revocation of the Certificate
4. Modification of information of the Certificate

### 4.9.5. Time within which CA Must Process the Revocation Request

Requests for CA certificate revocation from the GSSL CA is processed within seven (7) days of receipt, and the CA CRL(ARL) is published in the public repository.

Regarding Subscriber Certificate revocation the GSSL CA initiates revocation procedure immediately after receiving the request. After the revocation of the Certificate, the reflection of revocation to the CRL shall not exceed 24 hours. The GSSL CA investigates the facts and circumstances associated with the report and provides a preliminary report on its findings to the Subscriber or the entity that filed the problem report within 24 hours of after receiving the Certificate Problem Report.

After reviewing of the facts and circumstances, the GSSL CA cooperates with subscriber and entity reported the Certificate Problem Report or other revocation-related notices to determine whether the Certificate will be revoked or not, and if so, set the time within 24 hours to revoke the certificate. The period from receipt of the Certificate issue report or notice related to the revocation to the revocation of the Certificate shall not exceed the period specified in section 4.9.1.1, 4.9.1.2. The date of revocation selected by GSSL CA considers the following criteria.

- The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
- The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
- The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
- The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn’ t receive the goods they ordered); and
- Relevant legislation.

### 4.9.6. Revocation Checking Requirement for Relying Parties

Relying Parties are required to confirm the validity of each Certificate in the certificate chain by checking CRL or OCSP responder before relying on a GSSL Certificate.

### 4.9.7. CRL Issuance Frequency

The CA Certificate CRL(ARL) is updated at least every 364 days and within 24 hours after the CA certificate is revoked, and the value of the nextUpdate field does not exceed 12 months over the value of the thisUpdate field.

The Subscriber CRL is updated at least every day, and the value of the nextUpdate field does not exceed 10 days over the value of the thisUpdate field.

### 4.9.8. Maximum Latency for CRLs

The CA Certificate CRL(ARL) and Subscriber Certificate CRL are posted to the repository within one hour from generation.

### 4.9.9. On-line Revocation/Status Checking Availability

The GSSL CA supports Online Certificate Status Protocol(hereinafter the “OCSP” ) in issuing CA and Subscriber Certificates. OCSP addresses are:

- CA Certificate’s OCSP : ocsp-rca-ssl.gpki.go.kr
- Subscriber Certificate’s OCSP : ocsp-ca-ssl.gpki.go.kr

OCSP responses comply with RFC 6960. The GSSL CA issues a separate Certificate for signing OCSP responses. An OCSP Certificate signed by a CA contains an extension of the id-pkix-ocsp-nocheck type as defined in RFC 6960.

### 4.9.10. On-line Revocation Checking Requirements

The validity interval of OCSP response messages must be greater than or equal to eight (8) hours and less than or equal to ten (10) days. If the validity interval is less than 16 hours, the information must be updated prior to one-half of the validity period before the nextUpdate. If the validity interval is greater than or equal to 16 hours, the information is updated at least eight (8) hours prior to the nextUpdate and no later than four (4) days after the thisUpdate. An OCSP responder uses the GET method for requesting OCSP and receiving it. As for the CA Certificate, the OCSP response message should be updated at least every 12 months, and within 24 hours after the CA Certificate is revoked.

### 4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

### 4.9.12. Special Requirements re Key Compromise

If the Certificate private key of the CA is damaged, the GSSL CA immediately notifies the relevant authorities, such as the MOIS, the NIS, and other related entities.
If the Subscriber Certificate private key is compromised, the Subscriber must notify the GSSL CA that the Certificate is compromised.
The GSSL CA provides a way to report major damage via CA website.

### 4.9.13. Circumstances for Suspension

No stipulation.

### 4.9.14. Who Can Request Suspension

No stipulation.

### 4.9.15. Procedure for Suspension Request

No stipulation.

### 4.9.16. Limits on Suspension Period

No stipulation.

## 4.10. CERTIFICATE STATUS SERVICES

### 4.10.1. Operational Characteristics

CRL or OCSP operates to respond within 10 seconds. Revocation entries on a CRL or OCSP responses must not be removed until after the expiry date of the revoked Certificate.

### 4.10.2. Service Availability

Except for temporary unavailability due to maintenance and service failures, online CRL and OCSP services of all unexpired Certificates issued by CA shall be provided 24x7.

#### 4.10.3. Optional Features

No stipulation.

### 4.11. END OF SUBSCRIPTION

The CA ends the certification service and terminates the CA certificate by an official change notice of the Minister of the MOIS. Subscribers can end their Certificates as the following.

- If a Subscriber visits the website and applies for Certificate revocation, the certification service can be canceled.
- If a new Certificate is not issued or reissued after the Certificate expires, the Certificate service is canceled.

### 4.12. KEY ESCROW AND RECOVERY

No stipulation.

#### 4.12.1. Key Escrow and Recovery Policy Practices

No stipulation.

#### 4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

## 5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

### 5.1. PHYSICAL SECURITY CONTROLS

The GSSL CA facility is protected from physical threats such as intrusion or unauthorized access. Critical CA system tasks are performed in a physically secure zone with more than four (4) security layers, and physically separated from other systems so that only authorized personnel can access it.

#### 5.1.1. Site Location and Construction

The GSSL CA system is located in the Critical Information Infrastructure facility designated by the government and performs physical access control according to the national management regulations. Physical barriers (e.g., 3.0

T or more steel) are in place to shield electromagnetic wave emissions caused from system operation (e.g., key generation or authentication of CA Certificates) related to the Root CA.

### 5.1.2. Physical Access

An access control system is operated to control access to the control area by 2-Factor authentication (fingerprint recognition, vein recognition, etc.), and access rights are periodically reviewed. When entering the security area where CA facility is placed, the access date and time is recorded for audit trailing, and activities within the area are monitored by CCTV.

### 5.1.3. Power and Air Conditioning

A UPS system is operated to protect CA facility against blackouts and other electrical anomalies. Cables that support power, communication, data transmission, or services of the CA in the CA facility are protected from being blocked or damaged. An air conditioning system is operated to keep the temperature and humidity constant.

### 5.1.4. Water Exposures

The CA facilities are equipped with flood control facilities.

### 5.1.5. Fire Prevention and Protection

The CA facility is operated in a place equipped with fire detectors, portable fire extinguishers, and automatic fire extinguishing facilities in compliance with fire extinguishing regulations.

### 5.1.6. Media Storage

The Physical media access control is performed by storing the storage and recording media used in the CA service in the fireproof safe. It ensures all equipment containing storage media(fixed and removable disks) does not contain sensitive data prior to disposal. Storage media containing sensitive data shall be reset using methods which make existing data unrecoverable before disposal or reuse.

### 5.1.7. Waste Disposal

When each storage media that stores keys, activation data, critical files is discarded, it is processed according to internal procedures or destroyed completely.

### 5.1.8. Off-site Backup

The remote backup is performed for the CA service. The backup site maintains a level of security and control equivalent to the site where the main facility is installed.

## 5.2. PROCEDURAL CONTROLS

### 5.2.1. Trusted Roles

The operation manager designates and approves the Trusted Roles based on the principle of least privilege. The list of designated Trusted Roles is reviewed and updated at least once a year. For the security and reliability of the operation of the CA system, the roles listed below are separated, and there is no conflict of interest for each person. Trusted Roles are defined as follows.

- Management Manager : In charge of the overall CA tasks and approval of policies.
- Policy Administrator : In charge of policy establishment and amendment and performing training
- Security Manager: In charge of CA system security management
- Internal Auditor : In charge of CA system audit log review.
- Key Manager : In charge of key generation, transfer, and destruction procedures.
- Key Shareholder : In charge of performing M of N procedures during the key generation/transfer/destruction procedures.
- Fireproof safe Manager : In charge of HSM and backup management(fireproof safe at Main CA facility), remote backup management(DR facility)
- CA system Administrator: In charge of Certificate management(CA), Certificate Lifecycle, CRL, Administrator Certificate Management
- CA system Operator: In charge of server/DB/network Operation

- Subscriber Application Validator: In charge of validating and obtaining the application and identification documents regarding the Applicant Representative and domain validation.
- CA System Developer : In charge of Source code development and maintenance.

### 5.2.2. Number of Individuals Required per Task

At least three (3) people are required to activate the key for key generation, backup, storage, and recovery of the CA key.

### 5.2.3. Identification and Authentication for each Role

Each individual in a Trusted Role uses unique credential so that his/her identity can be verified by the CA system. Multi-Factor Authentication(hereinafter the “MFA” ) is applied to enter a security area and/or high-level security area.

### 5.2.4. Roles Requiring Separation of Duties

Responsibilities and tasks assigned to each individual in a Trusted Role is documented. In addition, the duties of the each individual in a Trusted Role must be separated based at the security-related aspects of the functions to be performed. Security Manager and internal auditors cannot take other Trusted Roles. Management manager and policy administrator do not perform CA system operation, Certificate management, or registration management roles.

## 5.3. PERSONNEL CONTROLS

The R&R(responsibilities and roles) assigned to the Trusted Role is documented, and separation of duties for the Trusted Role is implemented based on security concerns of the function to be performed.

### 5.3.1. Qualifications, Experience, and Clearance Requirements

Operating personnel is required to acquire IT-related qualifications recognized by the government or have work experience equivalent to them. Prior to participate in the Certificate management as an employee, representative, or independent contractor, the CA validates the identity and authenticity. The CA evaluates personnel assigned to the Trusted Roles, and shall be able to meet the performance requirement in his/her duties.

### 5.3.2. Background Check Procedures

Operating personnel is required to pass national background check. All employees must wear an identifiable identification card.

### 5.3.3. Training Requirements and Procedures

All personnel performing certification tasks must complete security regulations, internal management procedures, and technical training necessary to his/her duties. The contents of training are as follows.

- Information security (laws, regulations, manuals, etc.) and personal data protection training, etc.
- CA Operation procedures and roles and responsibilities of each person in charge
- TLS technology and training on the latest certification trend, etc.
- Training on the identity verification procedure and method for the person in charge

### 5.3.4. Retraining Frequency and Requirements

Personnel performing certification tasks complete security and related technical training every year.

### 5.3.5. Job Rotation Frequency and Sequence

No stipulation.

### 5.3.6. Sanctions for Unauthorized Actions

Personnel who engage in unauthorized actions are disciplined in accordance with relevant regulations and laws.

### 5.3.7. Independent Contractor Controls

No stipulation.

### 5.3.8. Documentation Supplied to Personnel

Personnel in trusted roles are provided with the internal documents necessary to perform their task.

## 5.4. AUDIT LOGGING PROCEDURES

Audit logging is implemented to monitor, detect, and report configuration changes related to the security of a CA system in a security support system under the control of a CA or a trusted third-party.

### 5.4.1. Types of Events Recorded

The CA system records the following events and records the Certificate management log according to the internal audit procedure.

1. CA and Key life cycle Management Records
   - Key generation, backup, storage recovery, migration, transfer, storage, and destruction
   - Certificate request, renewal, and revocation
   - Approval and rejection of Certificate requests
   - Cryptographic device life cycle management history
   - Creation of CRL and OCSP entries
   - Creation of a new Certificate profile and revocation of Certificate profiles

2. Subscriber Certificate life cycle Management Records
   - Certificate request and revocation
   - All verification activities specified in CA/Browser Forum Baseline Requirements and CA practices
   - Approval and rejection of Certificate requests
   - Certificate issuance
   - Creation of CRL and OCSP entries

3. Security records
   - Success and failure of CA system access attempts
   - Record of works related to CA and security system
   - Change security settings
   - Software installation, update, and removal for CA system

- System crashes, hardware failures, and other anomalies
- Firewall and router logs
- CA facility access record

4. All log records include:
- Log date and time
- ID of the subject generating the log
- Description of the log

### 5.4.2. Frequency of Processing audit Log

The log is reviewed once a month by a log auditor, and the log related to the CA key life cycle is reviewed on each quarter.

### 5.4.3. Retention Period for Audit Log

Logs are stored for two (2) years depending on types in consideration of storage space availability and management efficiency.

### 5.4.4. Protection of Audit Log

The GSSL CA implements procedures to safely protect stored data from threats including unauthorized modification and/or compromise of the integrity of the log until the audit log retention period expires.

- Only CA system Administrator and internal auditors have rights to access audit logs
- Modification or deletion of the audit logs is not allowed

### 5.4.5. Audit Log Backup Procedures

Logs shall be backed up in real-time, and a copy of the logs is stored in a safe off-site location.

### 5.4.6. Audit Collection System (internal vs. external)

Audit collection system is operated directly by the CA.

### 5.4.7. Notification to Event-causing Subject

The GSSL CA system is monitored by automated methods such as log analysis and event notification to notify important security events to operating personnel.

### 5.4.8. Vulnerability Assessments

The GSSL CA system is continuously monitored to external and internal vulnerabilities, and identifies the scope of the vulnerability evaluation scope, and performs the following risk assessments at least every year on a regular basis. When performing vulnerability assessment and penetration testing of the CA system and infrastructure, external personnel should be hired for independency and objectivity.

- Identify foreseeable internal and external threats that could lead to unauthorized access, disclosure, misuse, alteration, or destruction of Certificate data or Certificate management processes
- Evaluate the adequacy of policies, procedures, information systems, and technologies prepared by the CA to respond to these threats

For public and private IP addresses used in the CA system, a vulnerability scan shall be performed as follows.

- At least every three (3) months
- Within one (1) week after receiving the request from CA/Browser Forum
- When changing the system or network that the CA determines to be critical

The GSSL CA executes measures within 96 hours of a discovery of critical vulnerabilities with high risk. If not possible, the GSSL CA establishes action plan and countermeasures to mitigate vulnerabilities.

## 5.5. RECORDS ARCHIVAL

### 5.5.1. Types of Records Archived

As for the records to be archived, refer to items specified in section 5.4.1.

### 5.5.2. Retention Period for Archive

The GSSL CA retains all documents related to Certificate requests and Certificate revocation for at least two (2) years after those Certificates become invalid or revoked.

### 5.5.3. Protection of Archive

The GSSL CA manages backups archived at a distinct and separate location to prevent unauthorized changes, leakage, and destruction.

### 5.5.4. Archive Backup Procedures

The backup archives are utilized in the occurrence of loss or destruction of information in accordance with the backup and recovery procedures.

### 5.5.5. Requirements for Time-stamping of Records

All archived records are time-stamped using NTP(Network Time Protocol).

### 5.5.6. Archive Collection System (internal or external)

No stipulation.

### 5.5.7. Procedures to Obtain and Verify Archive Information

Information related to the CA system is requested through an official document in the name of the requesting organization after prior consultation with the GSSL CA. The GSSL CA replies to the request via an official document.

## 5.6. KEY CHANGEOVER

In the cases when CA key has expired or compromised, the procedure for providing a new CA Certificate to a Subject following a re-key is the same as the procedure for initial issuance of CA Certificate.

## 5.7. COMPROMISE AND DISASTER RECOVERY

### 5.7.1. Incident and Compromise Handling Procedures

The GSSL CA maintains controls to reasonable assurance that damage caused by security failures and malfunctions can be minimized through incident reporting and response procedures. In preparation for disaster, security failure, or business failure, the GSSL CA documents the business continuity and disaster recovery procedures to notify and protect affected Subscribers and Relying Parties. Procedures shall be in place to transfer relevant archival records to the responsible person. The business continuity plan is not subject to external disclosure. However, the internal auditor of the GSSL CA has rights to access the business continuity plan and security plan upon request. The GSSL CA  annually reviews and updates the business continuity plan, and conducts disaster recovery exercise according to the business continuity plan. The items to be included in the business continuity plan are as follows.

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of involved individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. A plan to maintain or restore the CA' s business operations in a timely manner following
interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and
activation materials) at an alternate location;
12. A definition of acceptable system outage and recovery times;
13. The frequency at which backup copies of essential business information and software are made;
14. The distance between CA sites; and
15. Procedures for securing an affected facility following a disaster and prior to restoring it either at the original or a different location.

### 5.7.2. Recovery Procedures if Computing resources, software, and/or data

**are corrupted**

The GSSL CA recovers data using archived data when critical data of Certification system is compromised or destroyed.

### 5.7.3. Recovery Procedures after Key Compromise

If the GSSL CA has recognized that private key of either CA or subscriber used in the certification service is not secure, it revokes those CA or subscriber certificates containing public keys and reissues certificates by generating new key pairs. In particular, once a Root CA private key is compromised, the GSSL CA informs browser vendors of the compromise and best estimate of the date of compromise.

### 5.7.4. Business Continuity Capabilities after a Disaster

According to the national business continuity guidance, the GSSL CA establishes and implements a business continuity plan to keep certificate life cycle tasks and CA facilities from being interrupted by disasters such as failures, terrorism, power outages, earthquakes, fires, and storm and flood, etc.

## 5.8. CA OR RA TERMINATION

When the certification authority is terminated, the GSSL CA notifies and takes the following measures to minimize the impact of the delegation termination.

- If a successor CA is designated, records related to service and operation are handed over
- Preserving all records described in this CPS for a minimum of one (1) year
- Revoking all Certificates issued by the CA no later than at the time of termination

# 6. TECHNICAL SECURITY CONTROLS

## 6.1. KEY PAIR GENERATION AND INSTALLATION

### 6.1.1. Key Pair Generation

The CA key is generated inside a HSM certified FIPS 140-2 Level 3 or higher. The generated private key cannot be extracted outside the HSM except for the purposes permitted by the GSSL CA. The Subscriber key pair is generated by the Subscriber. Requests for Subscriber Certificates are rejected if the Public Key does not meet the requirements in Sections 6.1.5 and 6.1.6 or if it has a Private Key that is known to be weak. At least three (3) of the designated personnel participate in key pair generation ceremonies of RootCA or CA and perform the task in the presence of internal or external auditors.

### 6.1.2. Private Key Delivery to Subscriber

The GSSL CA does not generate or archive Subscriber key pairs.

### 6.1.3. Public Key Delivery to Certificate Issuer

When issuing a CA Certificate, the CA submits a request for signing a CSR in PKCS#10 format to the GSSL Root CA.
The Subscriber submits a CSR in PKCS#10 format to the GSSL CA via the official website to which the TLS certificate is applied.

### 6.1.4. CA Public Key Delivery to Relying Parties

The CA public key is electronically signed by the GSSL Root CA. The GSSL CA provides chain validation procedures for Subscriber Certificates by posting Certificates of the Root CA and CA on the website.

### 6.1.5. Key Sizes

For the Certificate algorithm and key length, the Certificate must meet the following requirements. The Root CA Certificate, CA Certificate, and Subscriber Certificate must all meet the same requirements.

- Digest Algorithms : SHA-256, SHA-384 or SHA-512
- Minimum RSA Module Size (Unit: bits)

- Root CA Certificate : 4096
- CA Certificate : 3072
- Subscriber Certificate : 2048

### 6.1.6. Public Key Parameters Generation and Quality Checking

In the case of the RSA key, the GSSL CA confirms that the public exponent of the RSA key is an odd number of three (3) or more.

### 6.1.7. Key Usage Purposes(as per X.509 v3 Key Usage Field)

The cases where the Root CA private key is used to sign a Certificate is as follows.

- Self-signed Certificates to represent the Root CA itself
- CA Certificate
- Certificates for infrastructure purposes (e.g., Certificates for CA administrator, Certificates for internal CA operation devices, etc.)
- OCSP Response Verification Certificates

## 6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

### 6.2.1. Cryptographic Module Standards and Controls

The GSSL CA Key pairs are backed up and operated in HSM certified FIPS 140-2 Level 3 or higher.

### 6.2.2. Private Key (n out of m) Multi-person Control

The GSSL CA generates the CA key pair in accordance with an internal key generation procedure. At least three (3) of the designated personnel participate in key pair generation ceremonies.

### 6.2.3. Private Key Escrow

The GSSL CA does not escrow the CA key pair to a third-party.

### 6.2.4. Private Key Backup

The Root CA private key and CA private key is backed up and stored in a secure location according to the backup procedure. The backed-up private key is stored in an HSM and safely stored in a fireproof safe.

### 6.2.5. Private Key Archival

The GSSL CA does not separately archive CA private keys

### 6.2.6. Private Key Transfer into or from a Cryptographic Module

The Root CA private key and CA private key may be extracted according to a secure procedure specified by the HSM vendor under GSSL CA's approval for backup and recovery purposes.

### 6.2.7. Private Key Storage on Cryptographic Module

The private key of the GSSL CA is created and stored in the HSM that meets the requirements of section 6.2.1 of this CPS.

### 6.2.8. Activating Private Keys

The Root CA private key and CA private key stored in the HSM can be activated by multiple controls according to the procedure specified by the HSM vendor under the approval of the GSSL CA.

### 6.2.9. Deactivating Private Keys

The Root CA private key and CA private key stored in the HSM can be deactivated by multiple controls according to the procedure specified by the HSM vendor under the approval of the GSSL CA.

### 6.2.10. Destroying Private Keys

The CA private key may be destroyed for the following reasons.

- the Root CA or CA Certificate expired
- In case where there is a possibility that the private key of the CA has been compromised, leaked, or damaged

The GSSL CA can delete the private key stored in HSM by destroying the private key. Additionally, the GSSL CA can destroy backup tokens by zeroization of HSM according to the HSM specification. If zeroization or initialization fails, the equipment can be physically destroyed in a manner of removing the ability to extract the private keys.

### 6.2.11. Cryptographic Module Capabilities

A HSM that meets the requirements of section 6.2.1 must be used.

## 6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

### 6.3.1. Public Key Archival

CA and Subscriber Certificates are archived in accordance with backup procedures.

### 6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Certificates validity expires at the end of the validity period specified in the Certificate field. The maximum validity period of the issued Subscriber Certificate is 397 days.

## 6.4. ACTIVATION DATA

Hardware security module (HSM) activation key is stored in corresponding HSM and can be used by key administrators authorized by the GSSL CA.

Module activation for using a key pair in a HSM is performed according to a multiple controls procedure implemented with equipment that requires physical access control.

### 6.4.1. Activation Data Generation and Installation

Activation data is generated according to the specification of the HSM. This hardware security module is required to be certified for FIPS 140-2 Level 3.

### 6.4.2. Activation Data Protection

The procedure used to activate the HSM data depends on the HSM keypad(hereinafter the “PED”) and the access authentication key. The access authentication key is managed by a designated multiple controls procedure, and the PED is managed by a key manager.

### 6.4.3. Other Aspects of Activation Data

No stipulation.

## 6.5. COMPUTER SECURITY CONTROLS

### 6.5.1. Specific Computer Security Technical Requirements

CA system information of the GSSL CA is protected by server and OS control, physical control, and network control. Network security controls are specified in section 6.7.

Multi-factor authentication is applied to all accounts used for the Certificate life cycle management issued by the GSSL CA system.

- Permit access to authorized personnel to manage the CA system and ask for the responsibility for the CA system security
- Review all accounts in the system at least every three (3) months and deactivate the accounts that are no longer necessary for operation
- Restrict the access for a certain period if access attempts to the CA system fail more than five (5) times
- Retrieve the user's authority to the CA system within 24 hours once the job role changes or contract expires
- Apply MFA to all the CA systems that can be accessed from the security zone (including accounts that approve the equally applied to delegated third-parties for Certificate issuance)
- Apply Logout or session timeout when the workstation is no longer in use by the CA system-related administrator, operator, or person in charge
- Apply recommended security patch to the CA system within six months since its provided unless there is an evidence stating that the security patch causes additional vulnerabilities or instability outweighs the benefit of the security patch application

### 6.5.2. Computer Security Rating

No stipulation.

## 6.6. LIFE CYCLE TECHNICAL CONTROLS

### 6.6.1. System Development Controls

As for function changes or performance improvement of the Certification system, it is carried out under approval of the governing organization.

### 6.6.2. Security Management Controls

Separation of duties and least privilege principle must be applied to computers allowed to access the CA system. To access the GSSL CA system, it needs the approval of the CA. The rights to access are immediately withdrawn upon termination of duties.

### 6.6.3. life cycle Security Controls

No stipulation.

## 6.7. NETWORK SECURITY CONTROLS

The GSSL CA system is protected by the intrusion detection system and intrusion prevention system according to the network management policy and controls the specific port used to issue and validate the CA and Subscriber Certificates through the hardware firewall device.

1. Segment Certificate Systems into networks based on their functional or logical relationship
2. Apply equivalent security controls to all systems located in the same area with the CA system
3. Maintain Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks
4. Maintain and protect Issuing Systems, Certificate Management Systems, and Security Support Systems in at least a Secure Zone
5. Implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones and those on public networks
6. Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the GSSL CA has identified as necessary to its operations
7. Remove or disable all accounts, applications, services, protocols, and ports that are not used by the CA, and allow only the accounts, applications,

services, protocols, and ports authorized by the CA

8. Ensure that the CA’ s security policies encompass a change management process, following the principles of documentation, approval and review, and to ensure that all changes to GSSL CA systems
9. Grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System’ s security
10. Implement Multi-Factor Authentication to each component of the Certificate System that supports Multi-Factor Authentication
11. Change authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person’ s authorization to administratively access that account on the Certificate System is changed or revoked
12. Apply recommended security patches to Certificate Systems within six (6) months of the security patch’ s availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

### 6.8. TIME-STAMPING

The audit logs created by the Certificates, CRL, and other Certificate life cycles contain time information. The GSSL CA uses the NTP to synchronize system clocks at least once every eight (8) hours and all times are updated to the Universal Time Coordinated(hereinafter the “UTC” ) time zone.

# 7. CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1. Certificate PROFILE

The Certificate issued by the GSSL CA satisfies both RFC 5280 and CA/Browser Forum’s latest baseline requirements. If RFC 5280 and CA/Browser Forum Baseline Requirements are different, the CA/Browser Forum Baseline Requirements take precedence.

### 7.1.1. Version Number(s)

The CA and Subscriber Certificate issued by the GSSL CA is based on X.509 Version 3.

### 7.1.2. Certificate Content and Extensions; Application of RFC 5280

The Certificate issued by the GSSL CA uses the Certificate extension field specified in the “Appendix A. Certificate Profiles” and complies with CA/Browser Forum Baseline Requirements section 7.1.2 and technical standard RFC 5280.

### 7.1.3. Algorithm Object Identifiers

Certificate Algorithm OID uses the OID specified in the “Appendix A. Certificate Profiles” .

### 7.1.4. Name Forms

#### 7.1.4.1. Name Encoding

The encoded value of the Issuer DN field of all Certificates except for the Root CA Certificate must match the encoded value of the Subject DN field of the CA Certificate that issued the Certificate.

#### 7.1.4.2. Subject Information - Subscriber Certificates

By issuing the Certificate, the GSSL CA represents that it has conformed with the procedure specified in this CPS to verify that all subject information is accurate as of the date of Certificate issuance. The GSSL Certificate does not include a domain name in the Subject field, except as specified in section 3.2.2.4. The GSSL Certificate only contains information that is verified according to section 3.2 and does not include information that is not verified. The subject:organizationName, subject:localityName and subject:countryName attributes are verified according to section 3.2.2.1. The Subject attribute cannot use metadata such as ‘.’ , ‘-’ and ‘ ’ (i.e. space) characters by itself, and no other indications may be used if the value is missing, incomplete, or No stipulation. The GSSL CA will not issue Certificates containing reserved IP addresses or internal names in subjectAlternativeName field or subject:commonName attribute. Entries in dNSName must not contain the underscore character ( ‘_’ ) as they must be in the “Preferred name syntax” specified in RFC 5280.

#### 7.1.4.3. Subject Information – CA Certificates

The GSSL CA complies with the CPS and the CA/Browser Forum Baseline Requirements to ensure that all subject information is accurate as of the date of issuance of the Certificate. The subject:commonName attribute may be used as an identifier for the CA Certificate. The subject:commonName attribute of the GSSL CA Certificate must be unique. The GSSL Certificate includes the name of the CA in the subject:organizationName attribute. If it is a locally accepted abbreviation, it may contain somewhat different information, such as a verified name and a general variant or abbreviation. For example, if the official name is “Company Name Incorporated” , the GSSL CA may use “Company Name Inc.” or “Company Name” . The subject:countryName property contains the ISO 3166-1 country code identified in accordance with section 3.2.2.1.

### 7.1.5. Name Constraints

No stipulation.

### 7.1.6. Certificate Policy Object Identifier

The GSSL Certificate uses the CPS as the Certificate policy, and the related policy identifiers are as follows.

- Subscriber OV Certificate : 1.2.410.100001.100.1.2.2
- OCSP Certificate : 1.2.410.100001.100.1.3.2

The following policy identifiers assigned by the CA/Browser Forum are also used for Subscriber Certificates.

- OV Certificate : {joint-iso-itu-t(2) international-organizations (23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) organization-validated(2)} (2.23.140.1.2.2)

### 7.1.7. Usage of Policy Constraints Extension

No stipulation.

### 7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation.

### 7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

## 7.2 CRL PROFILE

CRLs issued by the GSSL CA comply with the RFC 5280 standard.

### 7.2.1. Version number(s)

All CRLs are issued as X.509 V2.

### 7.2.2. CRL and CRL Entry Extensions

- CRL Number : Use repe7ated monotonically increasing integer
- Authority Key Identifier : Same as the Subject Key Identifier of the Certificate
- Validity Date : UTC format (Optional)
- Reason Code : Reason for revocation (Optional)
  - keyCompromise(1)
  - affiliationChanged(3)
  - superseded(4)
  - cessationOfOperation(5)
  - privilegeWithdrawn(9)

## 7.3. OCSP PROFILE

OCSP responses conform with RFC 6960. The responses to OCSP requests are provided to the Authority Information Access via an OCSP responder URL. The OCSP responder does not respond with a “Good” for a Certificate that has not been issued. OCSP responses are signed by:

- the CA that issued the Certificates whose revocation status is being checked, or
- an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP

signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960).

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus MUST be present.

### 7.3.1 Version Number(s)

The GSSL CA OCSP response conforms with version 1 as defined in RFC 6960. In detail, the OCSP response may not include a random value in the response, even if the request contains a random value.

### 7.3.2 OCSP Extensions

No stipulation.

# 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

An annual audit is performed by an independent external auditor to assess compliance of GSSL CA with the WebTrust for CAs criteria. The audit report must meet CA/Browser Forum Baseline Requirements section 8.6.

## 8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The audit of the certification service is conducted at least once a year.

## 8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

Audits must be performed by a legal entity with the following qualifications and skills.

- Independence from the subject of the audit
- The capability and experience to process and audit against WebTrust or equivalent international certification audit standards
- proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and

security auditing, and the third-party attestation function
- In case of WebTrust Audit, a person licensed by WebTrust.org (WebTrust Practitioner)
- Bound by law, government regulation, or professional code of ethics
- Auditing agencies that maintain Professional Liability/Errors & Omissions insurance with a policy limit of at least one (1) million dollars in insurance coverage, except for internal government auditing agencies

## 8.3. ASSESOR'S RELATIONSHIP TO ASSESSED ENTITY

The auditor should not have a financial or business interest with the GSSL CA.

## 8.4. TOPICS COVERED BY ASSESSMENT

The annual audit is performed to validate that the CA service is appropriately performed by GSSL CA based on the WebTrust Audit Criteria and the CA/Browser Forum Baseline Requirements.

## 8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The GSSL CA take managerial and technical measures according to findings in the audit report.

## 8.6. COMMUNICATION OF RESULTS

An audit report covers the GSSL Certificate and related systems, policies, and procedures. The GSSL CA publishes audit report through its website. The GSSL CA is not required to disclose any general audit finding that does not affect the overall audit opinion.

The Audit Report contains at least the following clearly-labelled information:

- Name of the organization being audited
- The name and address of the organization performing the audit
- SHA-256 fingerprints of all Root CAs and CAs, including

Cross-Certificates

- The audit criteria(including version) used to audit each Certificate and associated key
- List of policy documents referenced when performing an audit (including versions)
- Whether the audit is an evaluation of a specific period or point in time
- The start and end dates of an audit period that includes a period of time
- A point in time date for a specific point in time
- The date the report was issued (Must be after the audit end date or the designated date)

## 8.7. SELF-AUDITS

The GSSL CA conducts self-audits at least once in a quarter basis for compliance with the CPS and CA/Browser Forum Baseline Requirements. Self-audit is conducted upon a sample randomly selected at least three (3)% of Certificates issued since the previous self-audit.

# 9. OTHER BUSINESS AND LEGAL MATTERS

## 9.1. FEES

### 9.1.1. Certificate Issuance or Renewal Fees

GSSL Certificate system is an information protection infrastructure operated by the government. It does not charge Subscribers for the issuance, re-key, and renewal of Certificates and other fees.

### 9.1.2. Certificate Access Fees

No extra fee is charged.

### 9.1.3. Revocation or Status Information Access Fees

No extra fee is charged.

### 9.1.4. Fees for Other Services

No extra fee is charged.

### 9.1.5. Refund Policy

No stipulation.

## 9.2. FINANCIAL RESPONSIBILITY

### 9.2.1. Insurance Coverage

None of the monetary indemnities is provided for the problems related to a GSSL Certificate.

### 9.2.2. Other Assets

No stipulation.

### 9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

## 9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

The GSSL CA observes applicable regulations on the protection of personal information deemed to be the confidential information by the relevant laws and CPS section 9.4.1.

### 9.3.1. Scope of Confidential Information

The GSSL CA keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel. The following information is considered confidential and protected against disclosure using a reasonable degree of care:

- Certificate application records and documents
- External or internal audit trail records and reports, except for WebTrust audit reports
- Emergency plans and Disaster Recovery Plans
- Private key

- Private key activation data
- Audit logs and archival records
- Personal information

### 9.3.2. Information Not Within the Scope of Confidential Information

Items specified in section 9.3.1 of the CPS are considered confidential information, and other information is considered public information. However, the registered Certificate and revocation information is not considered confidential information. Subscribers consent that the revocation data of all GSSL Certificates are public information and are posted every 24 hours. Subscriber application information marked as "Public" in Terms of Use or application submitted as part of the Certificate application information is published within the issued Certificate, so that such information does not fall within the scope of confidential information.

### 9.3.3. Responsibility to Protect Confidential Information

Confidential information on the GSSL Certificate is safely stored and managed by authorized personnel. The executives, employees, outsourcers, and contractors are responsible for protecting confidential information and have contractual obligations. All of these people must be trained in processing confidential information.

## 9.4. PRIVACY OF PERSONAL INFORMATION

### 9.4.1. Privacy Plan

The GSSL CA follows the Privacy Policy posted on the website when processing personal information. Personal information is only disclosed when the disclosure is required by law or when requested by the data subject of personal information.

### 9.4.2. Information Treated as Private

Personal information is collected and held in accordance with the Privacy Policy posted on the website.

### 9.4.3. Information Not Deemed Private

Information disclosed in Certificates, CRLs or OCSP is not deemed personal information.

### 9.4.4. Responsibility to Protect Private Information

The GSSL CA complies with related laws and regulations, such as the Personal Information Protection Act, and collects, holds, and processes personal information in accordance with the Privacy Policy posted on the website.

### 9.4.5. Notice and Consent to Use Private Information

The GSSL CA complies with related laws and regulations, such as the Personal Information Protection Act, notifies the use of personal information, and obtains consent of a data subject through the website and application document.

### 9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The GSSL Certificate Issuing System processes personal information of data subjects only within the scope specified in Section 9.4.2, and discloses personal information to third parties only if the disclosure is required under specifications of Articles 17 and 18 of the Personal Information Protection Act, such as the consent of the data subject and special provisions of the law.

### 9.4.7. Other Information Disclosure Circumstances

No stipulation.

## 9.5. INTELLECTUAL PROPERTY RIGHTS

All intellectual rights arising from the GSSL certification system belong to the MOIS.

### 9.5.1. Property Rights in Certificates and Revocation Information

The MOIS reserves the right to revoke certificates at any time and is responsible for maintaining the revocation information.

### 9.5.2. Property Rights in the Agreement

Participants in the GSSL service acknowledge that the MOIS holds all intellectual property rights to this CPS.

### 9.5.3. Property Rights of Names

The Subscriber reserves all rights to DN information, such as the authority name and domain included in the Subscriber Certificate.

### 9.5.4. Property Rights in Key Pairs

The Subscriber reserves all rights to the Subscriber's private and public keys.

## 9.6. REPRESENTATIONS AND WARRANTIES

### 9.6.1. CA Representations and Warranties

The GSSL CA makes no representations or warranties of the certification services provided except as specified in this CPS.

- Compliance with related domestic laws, decrees, regulations, enforcement rules
- Publishes and updates CRL and OCSP respond on a regular basis
- Compliance with the minimum requirements in this CPS and CA/Browser Forum Baseline Requirements
- Maintenance of online repository of public information on its website

### 9.6.2. RA Representations and Warranties

The GSSL CA does not operate external RA.

### 9.6.3. Subscriber Representations and Warranties

The GSSL CA requires the Applicant Representative to make an agreement and guarantee this item for the benefit of the CA and the recipient of the Certificate as part of the Subscriber Agreement or Terms of Use.

The GSSL CA collects one of the following for the explicit interests of certification agencies and Certificate recipients before issuing Certificates.

- Consent of the Applicant to the Subscriber Agreement

- Approval of the Applicant to the Terms of Use

The GSSL CA will implement a procedure to check whether the Subscriber Agreement or Terms of Use are legally applicable to the Applicant. In both cases, consent applies to Certificates issued at the request of Certificates. As long as each Certificate issued by the CA to the Subscriber is clearly subject to the application of the Subscriber Agreement or Terms of Use, separate consent can be obtained for each Certificate request or processed with a single consent for multiple Certificate requests and results.

The Subscriber Agreement or Terms of Use include the following obligations and guarantees imposed on the Applicant itself.

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
- Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that correspond to the Public Key to be included in the requested Certificate(s);
- Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- Reporting and Revocation: An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

- Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- Responsiveness: An obligation to respond to the CA's instructions concerning key compromise or Certificate misuse within a specified time period.
- Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

### 9.6.4. Relying Party Representations and Warranties

No stipulation.

### 9.6.5. Representations and Warranties of Other Participants

No stipulation.

## 9.7. DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN THIS CPS, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" . THE GSSL CA DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF ACCURACY OF INFORMATION PROVIDED WITH RESPECT TO CERTIFICATES ISSUED BY THE MOIS, THE CRL, AND ANY PARTICIPANT'S OR THIRD PARTY'S PARTICIPATION IN THE MOIS PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, THE CRL OR ANY OTHER GOODS OR SERVICES PROVIDED BY THE MOIS TO THE PARTICIPANT. EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1 OF THIS CPS, THE GSSL CA DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET

ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. THE GSSL CA DOES NOT GUARANTEE THE AVAILABILITY OF ANY PRODUCTS OR SERVICES AND MAY MODIFY OR DISCONTINUE ANY PRODUCT OR SERVICE OFFERING AT ANY TIME. A FIDUCIARY DUTY IS NOT CREATED SIMPLY BECAUSE AN INDIVIDUAL OR ENTITY USES SERVICES OF THE MOIS.

## 9.8. LIMITATIONS OF LIABILITY

GSSL CERTIFICATES ISSUED BY THE GSSL CA ARE OPERATED BY THE ELECTRONIC GOVERNMENT ACT AND ENFORCEMENT DECREE OF THE ACT, THEREFORE THE GSSL CA IS NOT RESPONSIBLE FOR ISSUES RELATED WITH THE USAGE OF A GSSL CERTIFICATE.

## 9.9. INDEMNITIES

No stipulation.

## 9.10. TERM AND TERMINATION

### 9.10.1. Term

This CPS is effective once it is published to the online repository.

### 9.10.2. Termination

The CPS and any amendments to the CPS remain in effect until it is replaced with a newer version.

### 9.10.3. Effect of Termination and Survival

The following rights, responsibilities, and obligations survive the termination of the CPS for Certificates issued under this CPS.

- All responsibilities and obligations related to confidential information, including those stated in section 9.3 of the CPS

- All responsibilities and obligations to protect private information, including those stated in section 9.4.4 of the CPS
- All representations and warranties, including those stated in section 9.6 of the CPS
- All limitations of liability are provided for in section 9.8 of the CPS

Even if this CPS is terminated, all Subscriber Agreements or Terms of Use remain in effect until the Certificate is revoked or expired.

## 9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Regarding this CPS, the GSSL CA mainly communicates with entities or individuals via email. The notification is considered valid as replied via e-mail. If the sender does not receive the email reply within five (5) days, the written notice shall be submitted to the following address.

- Korea Local Information Research & Development Institute, GSSL Center
- 301, Seongam-ro, Mapo-gu, Seoul, Republic of Korea (03923)
- E-mail: gssl@klid.or.kr

## 9.12. AMENDMENTS

In the case where the MOIS makes a significant change of policy, the latest version of the CPS is released using the new version number in the repository of the GSSL CA(ssl.gpki.go.kr/legal/cps). This CPS is updated at least once a year. In case of minor changes or error corrections that do not affect users and Certificates, the version number of the existing CPS can be maintained and modified without notifying users of the CPS.

### 9.12.1. Procedure for Amendment

Amendments to this CPS are made with the approval of the MOIS. The MOIS approves amendments to this CPS, and the GSSL CA publishes the amendments to the repository. Modifications may be updated, modified, or changed to this CPS, and details are described in the CPS. If there is a reason for minor changes or error corrections that are not related to the practices of the CPS, it may be modified without prior approval.

### 9.12.2. Notification Mechanism and Period

Amendments to the CPS of the GSSL are posted on the online repository to notify users.

### 9.12.3. Circumstances under which OID Must Be Changed

The MOIS is solely responsible for determining whether an amendment to the CPS requires OID changes of certificate policy.

## 9.13. DISPUTE RESOLUTION PROVISIONS

To the extent permitted by applicable law, Subscriber Agreement or Terms of Use shall contain a dispute resolution clause. The Disputes regarding GSSL certification system is subject to the decision of the Minister of the MOIS.

## 9.14. GOVERNING LAW

This CPS is governed, construed, and interpreted in accordance with the laws of the Republic of Korea. This particular jurisdiction's choice of law applies equally to providers, vendors, beneficiaries or other contractual relationships of GSSL implicitly or explicitly applicable to Certificates and services to ensure a comprehensive interpretation of this CPS regardless of location, place of use, and other products and services.

## 9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to the Electronic Government Act and related laws.

## 9.16. MISCELLANEOUS PROVISIONS

### 9.16.1. Entire Agreement

No stipulation.

### 9.16.2. Assignment

No stipulation.

### 9.16.3. Severability

No stipulation.

### 9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

### 9.16.5. Force Majeure

No stipulation.

## 9.17. OTHER PROVISIONS

No stipulation.

## Appendix A. Certificate Profiles

### 1. Root CA Certificate

| Fields | Req. | Value | |
|---|---|---|---|
| Version | (0x2) | 3 (0x2) | |
| Serial Number | CSPRNG random value of more than 8 byte | (Required) | |
| Signature Algorithm | SHA256 RSA | sha256WithRSAEncryption (1.2.840.113549.1.1.11) | |
| Issuer | Equivalent to Subject value | commonName = MOIS SSL Root CA<br>ogranizationName = Ministry of the Interior and Safety<br>countryName = KR | |
| Validity | 20 years | (Required) | |
| Subject | Mandatory Attributes CN, O, C | commonName = MOIS SSL Root CA<br>ogranizationName = Ministry of the Interior and Safety<br>countryName = KR | |
| Subject Public Key Info | RSA 4096 bit | Public Key Algorithm : rsaEncryption<br>RSA Public-Key : (4096 bit) | |
| Subject Key Identifier | Public Key Hash 20 byte | non-critical | (Required) |
| Key Usage | (0x06) | critical | keyCertSign, cRLSign (0x06) |
| Basic Constraints | Fixed Value | critical | Subject Type = CA<br>Path Length Constraint = None |

### 2. CA Certificate

| Fields | Req. | Value | |
|---|---|---|---|
| Version | (0x2) | 3 (0x2) | |
| Serial Number | CSPRNG random value of more than 8 byte | (Required) | |
| Signature Algorithm | SHA256 RSA | sha256WithRSAEncryption (1.2.840.113549.1.1.11) | |
| Issuer | Root CA Subject Value | commonName = MOIS SSL Root CA<br>ogranizationName = Ministry of the Interior and Safety<br>countryName = KR | |
| Validity | 10 years | (Required) | |
| Subject | Mandatory Attributes CN, O, C | commonName = MOIS SSL Server CA<br>ogranizationName = Ministry of the Interior and Safety<br>countryName = KR | |
| Subject Public Key nfo | RSA 3072 bit | Public Key Algorithm : rsaEncryption RSA Public-Key : (3072 bit) | |
| Authority Key dentifier | Root CA SKI Value | non-critical | (Required) |
| Subject Key Identifier | Public Key Hash 20 byte | non-critical | (Required) |

| | | | |
|---|---|---|---|
| Key Usage | (0x86) | critical | keyCertSign, cRLSign, digitalSignature (0x86) |
| Basic Constraints | Fixed Value | critical | Subject Type = CA<br>Path Length Constraint = 0 |
| Certificate Policy | CPS OID and URL(HTTP) | non-critical | [1]Certificate Policy: Policy<br>Identifier=anyPolicy<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://ssl.gpki.go.kr/legal/cps |
| Extended Key Usage | Fixed Value | non-critical | Server Authentication (1.3.6.1.5.5.7.3.1)<br>Client Authentication (1.3.6.1.5.5.7.3.2) |
| CRL Distribution Points | CRL URL (HTTP) | non-critical | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://ssl.gpki.go.kr/arl/SSL-RootCA.crl |
| Authority Information Access | Root CA Certificate and OCSP URL (HTTP) | non-critical | [1]Authority Info Access<br>Access Method=caIssuers (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ssl.gpki.go.kr/certs/ssl-rootca.cer<br>[2]Authority Info Access<br>Access Method=ocsp (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp-rca-ssl.gpki.go.kr |

## 3. Organization Validation Subscriber Certificate

| Fields | Req. | Value |
|---|---|---|
| Version | (0x2) | 3 (0x2) |
| Serial Number | CSPRNG random value of more than 8 byte | (Required) |
| Signature Algorithm | SHA256 RSA | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Issuer | CA Subject Value | commonName = MOIS SSL Server CA<br>ogranizationName = Ministry of the Interior and Safety<br>countryName = KR |
| Validity | Maximum of 397 days | (Required) |
| Subject | Attributes CN, O, L, S, C | commonName = (Domain Name Required)<br>ogranizationName = (Organization’ s English Name Required)<br>locality = (City/County/District,etc. Optional)<br>stateOrProvince = (State/Province,etc. Required)<br>countryName = KR |
| Subject Public Key nfo | RSA 2048 bit | Public Key Algorithm : rsaEncryption |

| | | | |
|---|---|---|---|
| | | RSA Public-Key : (2048 bit) | |
| Authority Key dentifier | CA SKI Value | non-critical | (Required) |
| Subject Key dentifier | Public Key Hash 20 byte | non-critical | (Required) |
| Key Usage | (0xA0) | critical | digitalSignature, keyEncipherment (0xA0) |
| Basic Constraints | Fixed Value | critical | Subject Type = End Entity<br>Path Length Constraint = None |
| Certificate Policy | CPS OID and URL(HTTP) | non-critical | [1]Certificate Policy:<br>Policy Identifier=1.2.410.100001.100.1.2.2<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://ssl.gpki.go.kr/legal/cps<br>[2]Certificate Policy:<br>Policy Identifier=2.23.140.1.2.2 |
| Subject Alternative Name | FQDN | non-critical | (Case1: for single domain)<br>DNS Name = Domain Name 1<br>or<br>(Case2: for multiple domain)<br>DNS Name = Domain Name 1<br>DNS Name = Domain Name 2<br>DNS Name = Domain Name 3<br>... |
| Extended Key Usage | Fixed Value | non-critical | Server Authentication (1.3.6.1.5.5.7.3.1)<br>Client Authentication (1.3.6.1.5.5.7.3.2) |
| CRL Distribution oints | CRL URL (HTTP) | non-critical | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=http://ssl.gpki.go.kr/crl/ca/Crl♯1p♯2Dp♯3.crl |
| Authority Information Access | CA Certificate and OCSP URL (HTTP) | non-critical | [1]Authority Info Access<br>Access Method=caIssuers (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://ssl.gpki.go.kr/certs/ssl-ca.cer<br><br>[2]Authority Info Access<br>Access Method=ocsp (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp-ca-ssl.gpki.go.kr |
| SCT List | more than 3 of CT logs | non-critical | (Required) |

## 4. OCSP Responder Ceritifcate Profile

○ CA Ceritifcate OCSP URL : http://ocsp-rca-ssl.gpki.go.kr

○ Subscriber Ceritifcate OCSP URL : http://ocsp-ca-ssl.gpki.go.kr

| Fields | Req. | Value | |
|---|---|---|---|
| Version | (0x02) | V3 (0x02) | |
| Serial Number | CSPRNG random value of more than 8 byte | (Required) | |
| Signature Algorithm | SHA256 RSA | sha256WithRSAEncryption (1.2.840.113549.1.1.11) | |
| Issuer | Issuer Subject Value | (Required) | |
| Validity | Maximum of 3 years | (Required) | |
| Subject | Required Attributes CN, O, C | (CA Ceritifcate  OCSP)<br>commonName = MOIS SSL CA OCSP Responder #(n)<br>(n = 1, 2, 3, ...)<br>ogranizationName = Ministry of the Interior and Safety<br>countryName = KR<br><br>(Subscriber Ceritifcate OCSP)<br>commonName = MOIS SSL Subscriber CA OCSP Responder #(n)<br>(n = 1, 2, 3, ...)<br>ogranizationName = Ministry of the Interior and Safety<br>countryName = KR | |
| Subject Public Key Info | RSA 2048 bit | Public Key Algorithm : rsaEncryption<br>RSA Public-Key : (2048 bit) | |
| Basic Constraints | Fixed Value | critical | Subject Type=End Entity<br>Path Length Constraint=None |
| Subject Key Identifier | Public Key Hash 20 byte | non-critical | (Required) |
| Authority Key Identifier | CA SKI Value | non-critical | (Required) |
| Key Usage | (0x80) | critical | Digital Signature (80) |
| Extended Key Usage | Fixed Value | non-critical | OCSP Signing (1.3.6.1.5.5.7.3.9) |
| Authority Information Access | OCSP URL (HTTP) | non-critical | (CA Ceritifcate  OCSP)<br>[1]Authority Info Access<br>Access Method=ocsp (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp-rca-ssl.gpki.go.kr<br><br>(Subscriber Ceritifcate OCSP)<br>[1]Authority Info Access<br>Access Method=ocsp (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp-ca-ssl.gpki.go.kr |

| | | | |
|---|---|---|---|
| OCSP No Revocation Checking | Fixed Value | non-critical | id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5) |