Government TLS Certification Authority Certification Practice Statement Version 1.0

Administrative Organization: National Development Council

Executive Organization: Chung Hwa Telecom Co., Ltd

June 14, 2019

Government TLS Certificate Authority Certificate Practice Statement

Version Revision Log

Version	Effective Date	Description of Revised Content
1.0	2019/06/14	Issue of first version

Contents

Summary

The following is a description of key aspects of the Government TLS Certification Authority Certification Practice Statement:

1. Certificate issuance:

   (1) Types: Government agency (organization) and unit organization validation (OV) SSL/TLS type server application software certificate.

   (2) Assurance level: The Government TLS Certification Authority (GTLSCA) issues assurance level 3 certificates defined by the certificate issuance policy in accordance with Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure assurance level 3 operations.

   (3) Scope of use: The SSL/TLS certificates issued by the GTLSCA primarily serve as a security mechanism for identification and provide the domain name and administration unit to relying parties to identify the subscriber's internet servers. The subscriber and relying parties only need to carefully use the certificates issued by the GTLSCA and exclude the scope of use restrictions and prohibitions of the GTLSCA CPS.

2. Major liability items:

(1) The GTLSCA assumes no liability for any consequences arising from the use of certificates by subscribers or relying parties outside of the scope of the GTLSCA CPS.

(2) Regarding liability for damages arising from the use of certificates by subscribers or relying parties, liability of the GTLSCA for damages shall be limited to that set down in relevant laws and regulations.

(3) The GTLSCA assumes no liability for any damages arising from a force majeure or other events not attributable to the GTLSCA.

(4) Unless otherwise stipulated by the law, the GTLSCA assumes the legal responsibility arising from registration work conducted by the RA.

(5) In the event that a relying party suffers damages due to provision of incorrect information by the subscriber, the subscriber shall assume sole legal responsibility.

(6) If a subscriber certificate must be revoked or reissued, the GTLSCA shall be immediately notified and relevant regulations of the GTLSCA CPS shall be followed. The subscriber shall bear legal responsibility for use of the certificate prior to the change.

3. Other important matters:

(1) In the event that the GTLSCA needs to temporarily halt part of

its certification services due to system maintenance, conversion or expansion, the GTLSCA will post a notice at the repository and notify subscribers. Subscribers and relying parties may not use this event as a reason to request compensation from the GTLSCA.

(2) If a subscriber or relying party suffers damages due to an error by the RA during examination, the RA shall assume responsibility for damage compensation according to the scope of liability set down in relevant laws and regulations.

(3) When a subscriber applies for a certificate, the GTLSCA shall provide the certificate content to the subscriber in advance for review. After the subscriber reviews the contents and finds it free of errors, the GTLSCA shall use this as a basis for certificate acceptance and issue the certificate. After the subscriber receives the certificate issued by the GTLSCA, the certificate shall be used in accordance with relevant regulations in the GTLSCA CPS.

(4) Subscribers and relying parties shall carefully select a secure computer environment and reliability application system. If the computer environment or application system infringes on the users' rights and interests, the subscriber or relying party shall be solely responsible.

(5) If the GTLSCA fails to operate normally due to certain circumstances, subscribers and relying parties shall quickly

look for other ways to complete their legal acts with other parties and the inability of the GTLSCA to operate normally shall not be used as a defense to others.

(6) Relying party acceptance of a GTLSCA issued certificate indicates understanding and agreement to the legal liability clauses of the GTLSCA and certificate use shall follow relevant regulations in the GTLSCA CPS.

(7) The NDC commissions a third party to conduct external compliance audits of the GTLSCA.

(8) Unless stipulated otherwise, if there is any inconsistency between the content of the modified version and original version of the GTLSCA CPS after the modifications take effect, the modified version shall prevail. If the modification is done by attached document and there is an inconsistency between the content of the attached document and the original version, the attached document shall prevail.

1 Introduction

The Government TLS Certification Authority Practice Statement (GTLSCA CPS) is formulated in accordance with the Certificate Policy for the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI), ITU-T X.509, request for comments such as RFC 3647 and RFC 5280) from the Internet Engineering Task Force, (IETF) and Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.

1.1 Overview

The Government TLS Certification Authority (GTLSCA) is a Subordinate Certification Authority of the Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) and the ePKI Root Certification Authority (eCA) issues certificates to the GTLSCA.

The GTLSCA is responsible for the issuance and administration of government agency (organization) and unit organization validation (OV) SSL / TLS type server application software certificates (SSL/TLS certificates).

The GTLSCA CPS delineates how GTLSCA acts in accordance with assurance level 3 in the CP to issue and manage certificates. The practice statements in the GTLSCA CPS is only applicable to GTLSCA-related entities such as GTLSCA, Registration Authority (RA), subscriber, relying party and repository.

The GTLSCA follows the official version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum (website: http://www.cabforum.org). As for effective date of each item of

information in the official version, the GTLSCA shall be in compliance (see Appendix 3). If GTLSCA CPS is in conflict with forum regulations such as with regard to SSL/TLS certificate issuance and management, the provisions announced by the CA/Browser Forum shall prevail.

The National Development Council (NDC) is the administrative organization of the GRCA. The establishment and any modification to the GRCA CPS may go into effect only after obtaining the permission of the eCA. The GTLSCA CPS is not authorized to be used by CAs outside the GTLSCA. The CA shall be solely responsible for any problems arising from the use of the CPS by other CA.

1.2 Document Name and Identification

1. Document name: Government TLS Certification Authority Certificate Practice Statement
2. Version: Version 1.0
3. Publication date: May 27, 2019
4. Downloading site: http://gtlsca.nat.gov.tw/download/GTLSCA_CPS_v1.0.pdf.
5. Certificate Policy Object Identifier (CP OID): id-cht-ePKI-certpolicy-class3Assurance、 {id-cht-ePKI-certpolicy 3}
6. CA/Browser Baseline Requirements CP OID：「2.23.140.1.2.2」

1.3 PKI Participants

The key participants of the GTLSCA are:

1. GTLSCA
2. Registration authority
3. Subscribers
4. Relying parties
5. Other related parties including contracted entities authorized by the NDC to establish, maintain and operate the system.

1.3.1 Certification Authorities

Responsible for government agency (organization) and unit SSL/TLS certificate issuance and administration work.

1.3.2 Registration Authorities

Responsible for collecting and verifying subscriber identity and registration work of certificate-related information. The Registration Authority (RA) is formed by a number of registration counters staffed by RA officers responsible for accepting registration and revocation applications. The RA should be audited

The RA server installed at the RA is responsible for verifying the identity of the RA officer and managing the registration counter. The RA administrator is responsible for managing the RA server. The RA administrator assigns account numbers and authorization levels for RA officers and issues IC cards to RA officers. A RA private key protected by RA private key signature is installed in the RA server for communication between the RA and the GTLSCA server.

1.3.3 Subscribers

GTLSCA subscribers refers to the entities in the certificate subject

name on issued certificates. For the GTLSCA, subscribers are the government agencies (organizations) and units on the SSL/TLS certificates approved for issue.

1.3.4 Relying Parties

A relying party is an entity that trusts the binding nature of the certificate subject name to a public key.

Prior to using the certificate issued by the GTLSCA, the relying parties must check the validity of the certificate being used based on the GTLSCA certificate and certificate status information. The relying party may use the certificate to identify the subscriber and its internet server name and establish secure communications between certificate subjects only after certificate validity is verified.

1.3.5 Other Participants

The contractor selected by NDC is responsible for the establishment, maintenance and operation of the GTLSCA system.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The SSL/TLS certificates issued by the GTLSCA primarily use secure sockets layer (SSL) and transport layer security (TLS) communication protocols to provide a secure mechanism for identity verification by the relying party of the subscriber’s internet server domain name and administration unit.

1.4.2 Prohibited Certificate Uses

1. Crime

2. Control of military orders for nuclear, biological and chemical weapons.

3. Operation of nuclear facilities.

4. Aviation and its control systems.

1.4.3 Certificate Usage Limitations

1. While using the private key, the subscriber must carefully select a secure computer environment and reliable application system to prevent infringement of its rights by malicious theft or misuse of the private key.

2. Prior to use of a GTLSCA issued certificate, relying parties shall check the certificate type and assurance level and determine if key usage meets requirements.

3. Relying parties shall make sure the critical and non-critical certificate extensions meet X.509 specifications.

4. Relying parties must follow GTLSCA CPS regulations.

1.5 Policy Administration

1.5.1 Organization Administering the Document

GTLSCA is responsible for establishing and administering the GTLSCA CPS.

1.5.2 Contact Person

The phone number, postal address and e-mail address of the GTLSCA can be found at https://gtlsca.nat.gov.tw.

1.5.3 Person Determining CPS Suitability for the Policy

The GTLSCA CPS must be reviewed by the NDC and then passed to the eCA for approval before external services are provided for issued certificates.

1.5.4 CPS Approval Procedures

Modifications to the CPS are handled in accordance with 1.5.3 CPS Examination and Approval regulations. Corresponding modifications shall be made to the GTLSCA CPS after certificate policy modifications are made and announced.

1.6 Definitions and Acronyms

See Appendix 1 Glossary and Appendix 2 English Acronyms.

2 Publication and Repository Responsibilities

2.1 Repositories

1. The repository shall publish the following information:

   (1) Issued certificates, CRL and other related certificate information.

   (2) Certificate policy and the GTLSCA CPS.

   (3) Latest external compliance audit results.

   (4) GTLSCA certificates (published until all certificates issued with the private key corresponding with the certificate's public key have expired).

   (5) Provide valid / expired and revoked SSL/TLS certificate websites as tested by application software vendor.

2. The repository provides 24 hour a day service. Website: https://gtlsca.nat.gov.tw.

3. Repository access controls are handled in accordance with section 2.4 Access Controls.

2.2 Publication of Certification Information

The GTLSCA uses the following means to publish certificate information:

1. Certificate Revocation List (CRL)

2. Offering Online Certificate Status Protocol (OCSP) inquiry services.

3. Repository certificate inquiry services.

2.3 Time or Frequency of Publication

1. The GTLSCA CPS may be published at the repository within 7 calendars after review and approval by the eCA.

2. The GTLSCA must issue and publish at least one CRL per day.

2.4 Access Controls on Repositories

1. The GTLSCA has established an information security protection mechanism that prevent external entities from directly connecting to internal servers.

2. Subscribers and relying parties use repository inquiry services and the repository server uses security controls to connect to the GTLSCA server database.

3. The GTLSCA only allows authorized personnel to administer the repository server.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

1. The subject name of certificates conforms to the distinguished name (DN) of ITU-T X.500.

2. The subject alternative name extension for subscription certificates must be non-critical extensions.

3.1.2 Need for Names to be Meaningful

1. Naming of certificate subject names shall comply with relevant government laws and regulations.

2. Certificate subject names and certificate subject alternative names must comply with Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and the Fully Qualified Domain Name shall be recorded in full.

3. The GTLSCA does not accept certificate applications with websites or IP addresses that have not been legally registered.

4. Certificate subject names shall include information for verification of organization identification contained in section 3.2.2 of the Organization Identity Authentication Procedure in the Organization Name field attributes.

5. A number of fully qualified domain names may be recorded in the certificate subject name column on one multiple domain certificate. Subscribers must possess the control rights to the domain name.

6. The universal domain certificate universal character (*) shall be placed on the far-left side of the fully qualified domain name. It is applicable to all website of the sub-domain.

3.1.3 Anonymity or Psuedonymity of Subscribers

The GTLSCA does not issue any anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Must comply with the name attribute definition of ITU-T X.520.

3.1.5 Uniqueness of Names

1. CA certificates

   CA certificate X.500 distinguished name:

   C=TW, O=Executive Yuan, CN= Government TLS Certification Authority- Gn

   Where n=1,2…

2. Subscriber certificate

   Subscriber certificates use the X.520 standard to define naming attributes. The certificate subject name format is as follows:

   - countryName(abbreviated as C)
   - stateOrProvinceName(abbreviated as S)
   - localityName(abbreviated as L)
   - organizationName(abbreviated as O)

- organizationalUnitName(abbreviated as OU)
- commonName(abbreviated as CN)
- serialNumber

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable.

3.1.7 Resolution Procedure for Naming Disputes

1. In the event of a dispute over subscriber name ownership, the dispute shall be resolved in accordance with relevant laws and regulations.
2. In the event of a dispute over domain name ownership, the dispute shall be resolved in accordance with internet competent authority procedures.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

1. For key pairs self-generated by the subscriber, the PKCS#10 certificate application file is generated by the key pair, affixed with a signature and passed to the RA.
2. The RA uses the subscriber’s public key to authenticate the application file signature to prove that the subscriber owns the corresponding private key.

3.2.2 Authentication of Organization Identity

3.2.2.1 Organization Identity Authentication

1. Regular applications

   The subscriber fills out the certificate application form and submits the application is official document form. The GTLSCA verifies the authenticity of the official document to prove the existence of the agency (organization) and unit and authorize the application.

2. Online applications

   Submit online application with valid government agency (organization) and unit certificate IC card. The RA verifies the digital signature with the certificate IC card to authenticate the subscriber identity and verify the existence of the agency (organization) and unit.

3.2.2.2 Domain Name Ownership Authentication

1. When the subscriber applies for a certificate, the GTLSCA follows the section 3.2.2.4 of the official version of the Validation of Domain Authorization or Control Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates from the CA/Browser Forum to select the recommended method to verify the domain applied for by the subscriber is registered and owned by the applicant and has control rights over the domain.

2. Domain names and organization ownership that are reviewed by certificate registration officers are international domain name

SSL / TLS certificates. If its dedicated fully qualified server name has a risky name, the SSL/TLS certificate is requested for additional comparison to prevent homomorphic spoofing attack of the international domain names.

3. Description of the domain validation methods that can be used:

(1) Validation using the government's Chinese /English domain name registration system:

Follow section 3.2.2.4.12 Validating the Applicant as a Domain Contact in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA / Browser Forum.

A. The competent authority of the GTLSCA also manages the allocation of government domains. When the subscriber applies for a certificate, the government's Chinese /English domain name registration system is used to verify the existence of the domain, registration and ownership by the applicant and control rights are possessed by the subscriber. Identity authentication is done in accordance with section 3.2.2 of the Organization Identity Authentication Procedure.

B. When a certificate is applied for the domain administered by the Ministry of Education (.edu), the Ministry of Education review counter authorized by the NDC verifies the domain was registered by the applicant and the subscriber possesses the control

rights and the GTLSCA conducts identity authentication in accordance with section 3.2.2 Organization Identity Authentication Procedure.

C. This method is also used for universal domain verification.

(2) Verification by domain contact email

Follow section 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum/ Email, Fax, SMS, or Postal Mail to Domain Contact.

A. The GTLSCA sends out an email containing a random value to the contact applying for domain registration. After the contact responds, the GTLSCA verifies whether the applicant has control over the fully qualified domain name.

B. The above random value shall be unique and have a validity of 30 days.

C. The GTLSCA may send a new email with an updated random value depending on the circumstances but the email's other content and recipient must be the same.

D. This method is also used for universal domain verification.

(3) Change through specific web content

Follow section 3.2.2.4.6 Agreed-Upon Change to Website in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.

A. The GTLSCA provides the specific web changes containing random values and the applicant must specific lists ("/.well-known/pike-validation") placed in the webpage content to verify the applicant possesses control rights over the fully qualified domain.

B. The validity period of the above random value may not exceed 30 days.

3.2.3 Authentication of Individual Identity

Not applicable.

3.2.4 Non-verified Subscriber Information

Unverified subscriber information may not be written on the certification.

3.2.5 Validation of Authority

1. When applying for a certificate, the subscriber shall follow section 3.2.2.1 Organization Identify Authentication and submit the application by official document or valid government agency (organization) and unit certificate IC card.

2. The GTLSCA shall verify ownership and possession of control rights over the domain name in accordance with section 3.2.2.2 Domain Name Ownership Authentication.

3.2.6 Criteria for Interoperation

Not applicable.

3.2.7 Data Source Accuracy

The GTLSCA shall evaluate the information accuracy. The following items shall be considered during the evaluation process:

1. Amount of time that the provided information has existed.
2. Updating frequency of the information source
3. Information provider and purpose of information collection.
4. Information availability.
5. Extent to which the information is publicly available.
6. Relative difficulty in forging or altering the information.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

When the key pair needs to be replaced after the subscriber's private key expires and a new application is submitted for a certificate, the GTLSCA shall follow the regulations in section 3.2 “Initial Registration”.

3.3.2 Identification and Authentication for Re-key after Revocation

When a subscriber applies for a new certificate due to certificate revocation, the GTLSCA shall follow the regulations in section 3.2 “Initial Registration”.

3.3.3 Certificate Extension Rekey

Subscriber certificates may not be extended.

3.4 Identification and Authentication for Revocation Request

For certificate revocation application authentication, follow the regulations in section 3.2 Initial Registration.

3.5 Certificate Suspension and Resumption Identification and Authentication

Subscribers may not submit certificate suspensions.

4 Certificate Life-cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Personnel authorized by government agencies (organizations).

4.1.2 Enrollment Process and Responsibilities

1. Verify the certificate applicant's identity before certificate issuance.
2. The certificate applicant shall provide identification documents.
3. Subscriber obligations are as follows:

   (1) Follow the GTLSCA CPS and subscriber terms and conditions and make sure the submitted application information is correct.

   (2) Make sure the information contained in the certificate is correct and follow the regulations in section 4.4 Certificate Acceptance Procedure during certificate acceptance. Immediate notify the RA if the information contained in the certificate is incorrect.

   (3) Follow the regulations in section 1.4.1 Certificate Usage during certificate use.

   (4) Properly keep and use its private key.

(5) If the certificate needs to be revoked, follow the regulations in section 4.9 Certificate Suspension and Revocation. The subscriber shall bear the relevant legal liability for use of the certificate prior to its revocation.

4.2 Certificate Application Processing

1. The certificate applicant submits the certificate application at the GTLSCA website.

2. The certificate applicant self-generates the key pair and uses the key pair to generate the PKCS#10 certificate application file, affixes the signature and uploads the certificate application file.

3. The certificate applicant sends the certificate application in official document form to the registration counter for processing.

4. If the SSL/TLS certificate is applied for online with an agency (organization) / unit certificate IC card, the application does not have to be submitted in official document form.

4.2.1 Performing Identification and Authentication Functions

The GTLSCA follows the identification and authentication procedure in section 3.2.2 Organization Identity Authentication Procedure as described below:

1. Subscriber identification and authentication

(1) After receiving the official document, the certificate officer follows the review guidelines to compare the official document number with the document issuing unit to perform identification, authentication and verify that the application has been authorized.

(2) If the SSL/TLS certificate is applied for online with an agency (organization) / unit certificate IC card, the RA verifies the digital signature for identification use.

2. Domain ownership authentication

(1) The GTLSCA only provides government agency (organization) and unit certificate applications and domain authentication shall be handled in accordance with section 3.2.2.2 Domain Name Ownership Authentication.

(2) The GTLSCA will regularly check the informantion about the phishing or fraudulent websites which are published by credible international organizations and make a domain blackist. The RAO must confirm the domain blackist to prevent misissued.

3. Certification Authority Authorization (CAA)

The GTLSCA shall check the domain name of the SSL/TLS certificate application case and whether there is a DNS resource record of the Certification Authority Authorization (CAA). The GTLSCA records the domain as「gtlsca.nat.gov.tw」in the CAA record and may issue the certificate under the following

circumstances:

(1) The GTLSCA is listed in the DNS resource record of the CAA as an authorized CA for SSL/TLS certificate issuance.

(2) No DNS resource record of the CAA.

(3) Not registered as an authorized CA for certificate issuance.

4.2.2 Approval or Rejection of Certificate Applications

After the GTLSCA completes application information review, identity verification and authentication, the certificate application may be approved.

The GTLSCA may refuse to issue a certificate under the following circumstances:

1. Fails to pass section 3.2.2 Organization Identity Authentication Procedure requirements.
2. The applicant had previously violated subscriber terms and conditions.
3. Other reasons to refuse issuance as determined by the GTLSCA.
4. The domain applied for by the subscriber is registered as a generic top-level domain for use by ICANN. The GTLSCA conducts domain comparison with related information from the www.icann.org website.

4.2.3 Time to Process Certificate Applications

1. The certificate registration counter shall the complete identity verification and information review procedure within two

working days provided the application information complies with relevant regulations.

2. After the certificate applicant assists in completing the domain verification, the GTLSCA completes certificate issuance work within one working day.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

1. After the GTLSCA and RA receives the certificate application information, the review procedures in the Chapter 3 Identification and Authentication Procedure regulations are followed. The certificate application review and issuance procedures are as follows:

   (1) The CA officer completes agency (organization) identity verification, domain name ownership authentication and CAA checking in accordance with section 3.2.2 Organization Identity Authentication Procedure and section 4.2.1 Implementation of Identity and Authentication Functions.

   (2) The subscriber prechecks the content of the issued certificates to make sure it is free of errors. After passing review, the GTLSCA issues the certificate and notifies the subscriber by email.

2. The precertificate generated by the GTLSCA in response to the certificate transparency mechanism may not be treated as a formal certificate issued by the GTLSCA.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

1. The certificate User is notified by email after certificate issuance.

2. The certificate user may check the certificate application progress at the CA website.

3. If approval is not given for certification issuance, the certificate user shall be notified by email or telephone and the reasons for the rejection shall be clearly explained.

4.4 Certificate Acceptance

1. The GTLSCA provides the certificate subject name and alternate subject name in advance to the certificate application for review.

2. After the certificate applicant checks if the content is correct and clicks accept certificate on the review page, the GTLSCA issues the certificate and announces it at the repository.

3. If the certificate applicant finds incorrect content on the certification, the GTLSCA or RA shall be notified immediately.

4. If the certificate applicant does not complete certificate acceptance work within 90 calendar days, the application case is deemed invalid and no announcement is made.

4.4.1 Conduct Constituting Certificate Acceptance

After the certificate applicant checks the certificate subject name and alternate name is free of errors and accepts the certificate, the GTLSCA

uses this as a basis for certificate acceptance.

4.4.2 Publication of the Certificate by the CA

The GTLSCA publishes the issued certificates on the repository or delivers the certificate to the subscriber by email to complete the certificate issuance work.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Certificates issued by the GTLSCA is published at the repository.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

1. Subscriber key pair generation complies with section 6.1.1 Key Pair Generation and the subscriber must have control rights over the private key.
2. The subscriber may not use the private key to issue certificates.
3. The subscriber shall protect the private key from unauthorized use or disclosure and make sure to use the private key for those key usages recorded in the certificate extension.
4. The subscriber must use the certificate in accordance with the CP and GTLSCA CPS regulations.

4.5.2 Relying Party Public Key and Certificate Usage

1. Relying parties must comply with GTLSCA CPS regulations during certificate use.

2. Relying parties shall use RFC conforming to ITU-T X.509 and IETF, and the software with standards or specifications of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.

3. Relying parties must verify the validity of the certificate including the certificate and the certificates of all CAs in the certificate chain.

4. Relying parties shall check issuing CA and subscriber certificate CP to determine the assurance level of the certificate.

5. Relying parties shall check the certificate usage.

4.6 Certificate Renewal

The GTLSCA does not offer certificate extension.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-key

Refers to new generation of a public and private key pair and use of original registration information to apply to the CA for certificate issuance.

4.7.1 Circumstance for Certificate Re-key

4.7.1.1 Circumstances under which a GTLSCA Certificate is Rekeyed

1. Expiry of the usage period of certificates issued with the private key.
2. GTLSCA certificate is revoked.

4.7.1.2 Circumstances under which a Subscriber Certificate is Rekeyed

1. Expiry of the subscriber private key usage period.
2. Subscriber certificate is revoked.

4.7.2 Who May Request Certification of a New Public Key

1. GTLSCA certificate rekey

   Personnel authorized by the GTLSCA submit subordinate CA certificate applications to the eCA.

2. Subscriber certificate rekey

   Personnel authorized by the government agency (organization).

4.7.3 Processing Certificate Re-keying Requests

1. The GTLSCA reapplied for the certificate in accordance with GTLSCA CPS regulations.

2. The subscriber shall follow section 4.1 Certificate Application and section 4.2 Certificate Application Procedure.

4.7.4 Notification of New Certificate Issuance to Subscriber

Follow regulations in section 4.3.2 GTLSCA Notification to Certificate Applicants.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

1. The GTLSCA conducts certificate rekey acceptance in accordance with the eCA's CPS regulations.

2. Subscribers perform certificate rekey acceptance in accordance with section 4.4.1 Certificate Acceptance Criteria regulations.

4.7.6 Publication of the Re-keyed Certificate by the CA

The GTLSCA publishes the completed rekeyed certificate at the

repository or transmits it by email to the subscriber.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The GTLSCA publishes the certificate to the repository after rekey.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

The GTLSCA does not allow subscribers to modify certificates.

4.8.2 Who May Request Certificate Modification

Not applicable

4.8.3 Processing Certificate Modification Requests

Not applicable

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable

4.8.6 Publication of the Modified Certificate by the CA

Not applicable

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.9 Certificate Revocation and Suspension

The GTLSCA provided 24 hour / 7 day certificate revocation service but does not provide certificate suspension service.

4.9.1 Circumstances for Revocation

1. The circumstances under which a subscriber can apply for certificate revocation:

   (1) Suspect or confirmed private key compromise.

   (2) Loss, theft, alteration, unauthorized disclosure or other damage or misappropriation of the private key.

   (3) Certificate no longer needs to be used.

   (4) Error or inaccuracy in the content recorded on the certificate.

   (5) The certificate is not authorized by the subscriber and the subscriber is not willing to backdate authorized when asked.

2. The GTLSCA may revoke a certificate under the following circumstances:

   (1) The GTLSCA private key or system spoofing, counterfeiting or compromise.

   (2) Content recorded on certificate is verified to be false or has undergone significant modification.

   (3) Misuse of the subscriber certificate.

(4) Subscriber signature-use private key spoofing, counterfeiting or compromise.

(5) Subscriber certificate does not comply with section 6.1.5 Key Size or section 6.1.6 Public Key Generation and Quality Check regulations.

(6) The GTLSCA did not issue subscriber certificate in accordance with CP, GTLSCA CPS or Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum regulations.

(7) Subscriber use of certificates did not comply with CP, GTLSCA CPS or Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum, user terms and conditions and relevant laws and regulations.

(8) Loss of usage rights for fully qualified domain name or IP address recorded on the subscriber certificate.

(9) The authorization or control verification method for the fully qualified domain name or IP address domain recorded on the subscriber certificate is untrustworthy.

(10) The domain recorded on the subscriber certificate is verified to have previously used a fake or misleading domain name.

(11) Universal domain certification is verified to have previously used a fake or misleading subordinate fully qualified domain name.

(12) The GTLSCA does not have certificate issuance rights and no longer provide repository, CRL or OCSP inquiry services.

(13) As per CP or GTLSCA CPS requirements.

(14) Verified to have used a subscriber private key vulnerable to disclosure which causes its compromise or allows subscriber public key calculations to obtain its corresponding private key.

(15) Verified flaws in the key generation method.

(16) Verified subscriber private key transmission to unauthorized person or agencies not under the jurisdiction of the subscriber.

(17) As notified by judicial authorities or prosecutors office.

(18) Notification by a higher authority or the competent authority of the subscriber.

(19) The GTLSCA may delay certification revocation in the event of a subscriber unique identifier name change (including a change of its higher authority). Notification of the grace period for certificate revocation shall be done separately.

4.9.2 Who Can Request Revocation

Certificate revocation applicants:

1. Subscribers
2. Higher authorities of the subscriber.
3. The GTLSCA (including RA).

Subscribers, relying parties, application software vendors and other third-party organizations may submit a certificate problem report to the GTLSCA. If one believes a certificate should be revoked, explain the reason for revocation in the report. The GTLSCA shall determine if the certificate revocation request is justified in accordance with section 4.9.3.3 Certificate Problem Reporting Mechanism.

4.9.3 Procedure for Revocation Request

4.9.3.1 Mechanism for Responding the Certificate Problems

The GTLSCA shall complete subscriber identity verification and authentication in accordance with the regulations in section 3.4 Certificate Revocation Application Identification and Authentication before revoking the certificate.

1. Subscriber certificate application revocation

   (1) The subscriber goes to the GTLSCA website, fills out a certificate revocation application and sends to the certificate revocation application in official document form to the registration counter.

(2) The certificate registration officer completes the subscriber identity verification and authentication in accordance with the regulations in section 3.4 Certificate Revocation Application Identification and Authentication and checks the accuracy of the certificate revocation application.

(3) After the certificate revocation application is reviewed, the GTLSCA shall complete the certificate revocation work within one working day.

2. GTLSCA revocation

The certificate may be revoked after the certificate is checked by a registration officer.

4.9.3.2 Publication and Notification

1. The revoked certificate is added to the CARL and the certificate status information is published at the repository before the next publication of the CARL at the latest and until the revoked certificate expires.

2. The GTLSCA may notify the applicant of the certificate revocation application results by email, phone or official document.

4.9.3.3 Certificate Problem Reporting Mechanism

1. The person who discovered the problem reports the certificate problem to the email address provided in section 1.5.2 Contact Information.

2. The GTLSCA accepts certificate problem reports and provides certificate problem replies 24/7.

3. The GTLSCA shall provide a preliminary investigation report to the subscriber and the person who discovered the problem within 24 hours after receiving the certificate problem report.

4. The GTLSCA shall jointly discuss the problem with the person who made the discovery. If the certificate needs to be revoked, the certificate revocation date shall be evaluated and selected based on the following criteria.

   (1) Content of reported problem (scope, content, severity, importance and hazard risk)

   (2) Certificate revocation effects (direct and indirect effects on the subscriber and relying parties)

   (3) Number of certificate problems submitted for the certificate or by the subscriber.

   (4) Unit or personnel who submitted the certificate problem.

   (5) Related legal provisions.

The processing period for GTLSCA after acceptance of the certificate problem report or receiving certificate revocation notification is determined based on the regulations in section 4.9.5 GTLSCA Processing Period for Certificate Revocation Requests.

4.9.4 Revocation Request Grace Period

Refers to the time in which the certificate revocation request must be submitted after the certificate revocation circumstances are verified.

1. When GTLSCA's own certificate needs to be revoked, the eCA must be notified within one hour.

2. When a subscriber's certificate needs to be revoked, the certificate revocation request must be submitted within 10 working days at the latest. The GTLSCA may extend the certificate revocation grace period depending on the circumstances.

4.9.5 Time within Which CA Must Process the Revocation Request

In principle, the GTLSCA shall complete certificate revocation work within 5 calendar days after acceptance of the certificate revocation request. However, certificate revocation must be completed within one calendar day under the following circumstances:

1. The subscriber submits the certificate revocation request to the GTLSCA.

2. The subscriber notifies the GTLSCA and reports that the original certificate request was unauthorized and reauthorization will not be given.

3. The GTLSCA verifies subscriber private key spoofing, counterfeiting or compromise.

4. The GTLSCA verifies the domain authorization or control verification method for the fully qualified domain name is the untrustworthy.

4.9.6 Revocation Checking Requirement for Relying Parties

Before the certificate is issued by the GTLSCA, relying parties shall

first check the CRL or OCSP reply message published by the GTLSCA to verify the validity of the certification and correctness of the certificate chain.

4.9.7 CRL Issuance Frequency

1. CRL are issued at least once per day with a valid period of not less than 36 hours.

2. The GTLSCA must reissue the CRL after certification revocation work is completed.

4.9.8 Maximum Latency for CRLs

The GTLSCA shall publish the next CRL prior to the next update time recorded on the CRL.

4.9.9 On-line Revocation/Status Checking Availability

1. The GTLSCA provides certificate inquiry and download, CRL and OCSP inquiry services.

2. The GTLSCA provides OCSP response messages conforming to RFC 6960 and RFC 5019 specifications from the Online Certificate Status Protocol Responder (OCSP Responder).

3. The GTLSCA uses its signature-use private key to issue RSA 2048 w/SHA-256 OCSP responder certificates.

4. The OCSP responder certificate must include the extension field 「id-pkix-ocsp-nocheck」 in compliance with RFC 6960 specifications.

4.9.10 On-line Revocation Checking Requirements

1. Relying parties must verify the certificate validity using the CRL or OCSP inquiry service.

2. Subscribers can at least use the HTTP GET method to execute the OCSP inquiry service.

3. The updating frequency of certificate status information is at least one update every four days. The maximum validity period for response messages is 10 calendar days.

4. For certificates that have not yet been issued, OCSP inquiry services may not reply that its status is ‘good’.

4.9.11 Other Forms of Revocation Advertisements Available

1. The GTLSCA supports OCSP stapling according to RFC 4366 specifications.

2. If the subscriber uses the above protocol to conduct certificate status inquiries, the GTLSCA shall use subscriber terms and conditions or technical inspection methods to ask the subscriber to initiate OCSP stapling.

4.9.12 Special Requirements Related to Key Compromise

Not stipulated

4.9.13 Circumstances for Suspension

Use of SSL/TLS certificates may not be suspended in accordance with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates regulations issued by CA/Browser Forum.

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.9.17 Procedure for Certificate Resumption

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The certificate revocation information in the CRL or OCSP reply message may only be removed after the revoked certificate has expired.

4.10.2 Service Availability

1. The GTLSCA provides 24/7 uninterrupted repository service. The certificate status inquiry service response time must be less than 10 seconds.

2. If the repository service is not functioning properly, normal operation must be resumed within two working days.

3. The GTLSCA has a 24/7 response mechanism to handle high priority certificate problem reports.

4.10.3 Optional Features

Not stipulated

4.11 End of Subscription

Refers to certificate subscribers that no longer use GTLSCA services. The criteria for GTLSCA to give permission to the subscriber to suspend service are:

1. Expiry of the certificate.
2. Revocation of the certificate by the subscriber.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

1. GTLSCA signature-use private keys cannot be escrowed.
2. GTLSCA does not support subscriber private key escrow and recovery.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The GTLSCA does not support session key encapsulation and recovery.

5 Facility, Management, and Operation Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The GTLSCA facility is located in Data Communacation Building, No. 21, Sec. 1, Xinyi Rd., Zhongzheng Dist., Taipei City 100, Taiwan (R.O.C.). The facilities possess physical security mechanisms including access control, security, intrusion detection and video surveillance.

5.1.2 Physical Access

1. The GTLSCA operates in accordance with assurance level 3 physical controls which include:

   (1) Main entrance and building security guards.

   (2) Access control system.

   (3) Fingerprint recognition system.

   (4) Cabinet surveillance system.

2. Portable storage media must be checked and verified to be free of computer viruses and any malicious software.

3. Non-GTLSCA personnel entering and leaving the facility are required to sign the entry/exit log and must be accompanied throughout by GTLSCA personnel.

5.1.3 Power and Air Conditioning

1. The power system for the facility includes municipal power, an electric generator (holding enough fuel for six days of continuous operation) and an uninterrupted power system which can provide at least six hours of backup power.

2. The facility has a constant temperature and humidity system.

5.1.4 Water Exposures

The facility is located at the third or higher floor of the building. This building has a water gate and water pump protection.

5.1.5 Fire Prevention and Protection

The GTLSCA facility has an automatic fire detection and alarm system with self-activating extinguishing equipment and manual switches are installed at every major entrance / exit of the facility.

5.1.6 Media Storage

Audit records, archives and backups are kept in storage media. Besides the one copy kept at the GTLSCA facility, another copy is made and kept at a secure location off-site.

5.1.7 Waste Disposal

Media used for storage of sensitive information that is no longer being used by the GTLSCA shall be destroyed in accordance with the information security regulations announced by relevant government agencies or other ways premited by NDC.

5.1.8 Off-Site Backup

1. The off-site backup site is located in Taichung which is over 30 km away from the GTLSCA facility.

2. The backup content includes data and system programs. At least one data backup is performed each month.

3. The off-site backup system and main system have identical security levels.

5.2 Procedural Controls

Identification and authentication of each trusted role is done according to the tasks they perform to ensure the security of work procedures.

5.2.1 Trusted Roles

1. The five GTLSCA trusted roles are administrator, officer, auditor, operator and controller. The tasks performed by these roles are as follows:

   (1) The administrator is responsible for:

   - Installation, configuration and maintenance of the GTLSCA system.
   - Creation and maintenance of GTLSCA system user accounts.
   - Setting of audit parameters.
   - Generation and backup of GTLSCA keys.

(2) The officer is responsible for:

- Initiation or termination of certificate issuance service.
- Initiation or termination of certificate revocation service.

(3) The auditor is responsible for:

- Checking, maintenance and archiving of audit logs.
- Conducting or supervising internal audits.

(4) The operator is responsible for:

- Operation and maintenance of system equipment.
- System backup.
- Storage media updating.
- Software and hardware updates outside the certificate management system.
- System abnormality and network security event reporting.

(5) The physical security controller is responsible for:

- System physical security control.

2. Personnel controls of each trusted roles is done in accordance with the regulations in section 5.3 Personnel Controls.

3. Each trusted role may be performed by a number of persons but one person shall be appointed to the chief role.

5.2.2 Number of Persons Required per Task

The number of people required for each task is as follows:

1. Administrator: At least 3 qualified individuals are needed.
2. Officer: At least 3 qualified individuals are needed.
3. Auditor: At least 2 qualified individuals are needed.
4. Operator: At least 2 qualified individuals are needed.
5. Physical security controller: At least 2 qualified individuals are needed.

The number of people assigned to perform each task is as follows:

Task	Administrator	Officer	Auditor	Operator	Physical Security Controller
Installation, configuration and maintenance of the GTLSCA system	1				1
Establishment and maintenance of GTLSCA certificate management system user accounts	1				1
Set audit parameters	1				1
Generation and backup of GTLSCA keys	2		1		1
Initiation or termination of certificate issuance service.		2			1
Initiation or termination of certificate revocation service		2			1
Checking, maintenance and archiving of audit logs			1		1
Daily operation and maintenance of system equipment				1	1

Task	Administrator	Officer	Auditor	Operator	Physical Security Controller
System backup				1	1
Storage media updating				1	1
Software and hardware updates outside the certificate management system				1	1

5.2.3 Identification and Authentication for Each Role

1. User account numbers, passwords and IC cards are used by the GTLSCA to identify and authenticate administrator, officer, auditor and operator roles.

2. A central access system is used to identify and authenticate the physical security controller role.

5.2.4 Roles Requiring Separation of Duties

Role assignment must comply with the following rules:

1. The administrator, officer and auditor roles may not be concurrently held.

2. The physical security controller may not concurrently assume any of the other four trusted roles.

3. A person serving a trusted role is not allowed to perform self-audits.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance

Requirements

1. Security checks must be done before personnel selection and employment.

2. Evaluation management must be done for personnel at regular intervals.

3. Regular instruction and training must be held for personal at regular intervals.

4. Personnel must sign and abide by the confidentiality agreement.

5.3.2 Background Check Procedures

1. GTLSCA work personnel must undergo qualification, experience and background checks by GTLSCA and personnel department supervisor based on their trusted role.

2. The job characteristics, duties performed and experience of each trusted role shall be reviewed each year to determine if the individual is suitable for the role.

5.3.3 Training Requirements

The education and training requirements of each trusted role is as follows:

Trusted role	Education and training requirements
Administrator	1. GTLSCA security certification mechanism 2. Operation procedure for the installation, configuration and maintenance of the GTLSCA system. 3. Establishment and maintenance of operation procedures for system user accounts. 4. Operation procedure for audit parameter configuration. 5. Operation procedure for GTLSCA key generation and backup.

	6. Post-disaster recovery and continuous operation procedure.
Officer	1. GTLSCA security certification mechanism 2. Certificate issuance operation procedure 3. Certificate revocation operation procedure 4. Post-disaster recovery and continuous operation procedure
Auditor	1. GTLSCA security certification mechanism 2. GTLSCA audit system use and operation procedure 3. Audit log checking, upkeep and archiving procedure 4. Post-disaster recovery and continuous operation procedure
Operator	1. System backup operation procedure 2. Maintenance procedure for the daily operation of system equipment 3. Storage media updating procedure 4. Post-disaster recovery and continuous operation procedure
Physical security controller	1. Physical access authorization setting procedure 2. Post-disaster recovery and continuous operation procedure

5.3.4 Retraining Frequency and Requirements

1. Education and training are held annually for each trusted role.
2. When there are hardware / software upgrades, work procedure changes, equipment replacement and amendments to related regulations.

5.3.5 Job Rotation Frequency and Sequence

1. Administrators may be reassigned to the position of officer or auditor after departure from their original position for one full year.
2. Officers may be reassigned to the position of administrator or auditor after departure from their original position for one full year.
3. Auditors may be reassigned to the position of administrator or officer after departure from their original position for one full year.

4. Only operators with two full years of experience who have received the requisite training and passed review may be reassigned to the position of administrator, officer or auditor.

5.3.6 Sanctions for Unauthorized Actions

The GTLSCA shall take appropriate administrative and disciplinary actions against personnel who have committed violations of the relevant regulations. In the event of serious violations that have resulted in damages, appropriate legal action shall be taken.

5.3.7 Independent Contractor Requirements

Contract personnel must sign a confidentiality agreement and perform work in accordance with regulations.

5.3.8 Documentation Supplied to Personnel

The GTLSCA shall provide the CP, technical specifications, this CPS, system operation manuals and documents related to the Electronic Signature Act to relevant personnel.

5.4 Audit Logging Procedures

1. Security audit logs shall be kept for all security-related events and these logs shall be immediately available when audits are performed.

2. Security audit logs may be automatically generated by the system or manually recorded in paper form.

5.4.1 Types of Events Recorded

1. Security audit

- Changes to key audit parameters.
- Any attempts to delete or alter audit logs.

2. Identification and authentication
   - Successful or failed attempt to set up a new role
   - Administer changes the maximum number of identity verification attempts allowed
   - Failure to log into the system
   - Account number locked out
   - Change in the identity verification mechanism of the system
3. GTLSCA key generation (not including generations of single use)
4. GTLSCA private key access
5. Addition, deletion or storage of a public key
6. Private key export other than single use keys
7. Certificate registration, revocation and status change application procedure
8. Security-related configuration setting changes
9. Account number addition, deletion and access authorization modifications
10. Certificate profile change
11. CRL profile change

12. GTLSC server setting change

13. Physical access and site security

14. Anomalies

5.4.2 Frequency of Processing Log

The GTLSCA performs one audit log check per month and tracks and investigates major events.

5.4.3 Retention Period for Audit Log

Audit logs are kept for two months. At the end of the retention period, audit personnel remove the information. Substitute personnel may not perform this task.

5.4.4 Protection of Audit Log

1. Use signature and encryption technology to store audit logs and use non-modifiable storage media.

2. The private key used to sign event logs must not be used for other purposes.

3. The audit system’s private key shall have security protection measures.

4. The audit logs must be kept in a secure location.

5.4.5 Audit Log Backup Procedures

1. Electronic audit logs are backed up once per month.

2. The audit system performs daily, weekly and monthly automatic archiving of audit logs.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system is established internally in the GTLSC system. The audit procedure is initiated when the GTLSC system is activated.

In the event that the automatic audit system cannot work normally and system information is in a high-risk state, the GTLSC shall suspend certificate issuance service and only resume service after the problem is solved.

5.4.7 Notification to Event-causing Subject

The audit system does not need to notify the event-causing entity if the events that have recorded by the audit system.

5.4.8 Vulnerability Assessments

The GTLSCA conducts risk assessments of the operating system, physical facilities, certification management system and network annunally.

5.5 Records Archival

5.5.1 Types of Records Archived

1. Relevant information obtained by GTLSCA from the eCA certificate application.
2. CPS
3. Important contracts
4. System and equipment configurations。
5. System and configuration modifications or updates

6. Certificate application information
7. Revocation application information
8. Certificate acceptance confirmation records
9. Token activation records
10. Issued or published certificates
11. GTLSC rekey records
12. Issued or published CRL
13. Audit logs
14. Other explanatory information or application program used for the verification and authentication of archived information.
15. Documents requested by audit personnel.
16. Organization and individual identity verification defined in section 3.2.2 Organization Identification and Authentication Procedure and section

5.5.2 Retention Period for Archive

1. The retention period for archived records and the application programs used to process file records is 10 years.
2. Written information shall be destroyed in a safe manner at the end of archived record retention period. Information in electronic form must be backed up in other storage media. Suitable protection must be provided or the information must be destroyed in a safe manner.

5.5.3 Protection of Archive

1. Archived records may not be amended, modified or deleted.
2. Archived records may be transferred to another storage media but the protection level may not be lower than the original protection level.
3. Archived records shall be kept is a secure location.

5.5.4 Archive Backup Procedures

1. Archived electronic records shall be backed up at the off-site backup.
2. Paper records will be regularly archived by personnel who is authorized.

5.5.5 Requirements for Time-stamping of Records

1. For records archived in electronic form, the timestamping information on each record shall include date and time information and use suitable digital signature protection which can be used to check the date and time information on the record for alteration.
2. The date and time information on the electronic records is the date and time of the computer operating system and not the electronic timestamping information provided by a third party.
3. Calibration of all GTLSCA computer systems must be performed at regular intervals.
4. Time information shall be recorded when necessary on archived written records containing date information. Alterations of date

and time information on records must by confirmed by signature of audit personnel.

5.5.6 Archive Collection System (Internal or External)

The GTLSCA does not have an archived record collection system.

5.5.7 Procedures to Obtain and Verify Archive Information

1. Archived records may be obtained after a written application is submitted and permission is received

2. Audit personnel are responsible for verification of archived records. The authenticity of signatures and dates on written documents must be verified and the digital signatures on archived records must be verified for electronic files.

5.6 Key Changeover

1. The GTLSCA may replace the key pair used to issue certificates and obtain a subordinate CA certificate issued by the eCA prior to the expiry of the private key's certificate use period.

2. Subscriber private keys are replaced in accordance with the regulations in section 6.3.2 Public and Private Key Use Periods. The regulations in section 4.2 Certificate Application Procedure shall be followed for subscriber rekey and certificate applications.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The GTLSCA has set up reporting and handling procedures in the event of an emergency or system compromise and hold annual drills that

follow this procedure.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

The GTLSCA has set up recovery procedures for computer resource, software and data corruption and holds annual drills that follow this procedure.

If the computer equipment is damaged or unable to operate, priority shall be given to restoring repository operation and rapidly reestablishing certificate issuance and management capabilities.

5.7.3 Entity Private Key Compromise Procedures

The GTLSCA has set up a signature key compromise recovery procedure and holds annual drills that follow this procedure.

5.7.4 Business Continuity Capabilities after a Disaster

1. The GTLSCA Exercise the Disaster recovery drill annually.
2. In the enent of disaster, GTLSCA will prioritize the operation of repository and rebuild other functions of GTLSCA.

5.7.5 GTLSC Revoked Signature Key Certificate Recovery Procedure

The GTLSC has set up a revoked key certification recovery procedure and holds annual drills that follow the procedure.

5.8 CA or RA Termination

1. Except for those who cannot be notified, the GTLSCA shall notify all subscribers with unrevoked and unexpired certificates

and publish the notice at the repository three months prior to the scheduled service termination date.

2. All valid certificates are revoked. Safekeeping and transfer work for file records is performed.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 GTLSCA key pair generation

1. The GTLSCA generates key pairs within the hardware cryptographic module in accordance with the regulations in section 6.2.1 Cryptographic Module Standards and Controls. The key generation process uses FIPS140 compliant random number generators and RSA key algorithms.

2. Private key output and input are performed in accordance with the regulations in section 6.2.2 Key Multi-Person Control and 6.2.6 Private Key Transfer into and from a Cryptographic Module.

3. A key generation script must be prepared and followed during key generation. Key generation is performed while being witnessed GTLSCA-related personnel and a qualified auditor and a video of the key generation process is kept.

4. The qualified auditor shall issue a key generation ceremony witness report to confirm that the GTLSCA key generation process has followed the key generation script and control measures in order to ensure the integrity and confidentiality of the key pair.

6.1.1.2 Subscriber Key Pair Generation

The subscriber must self-generate the key pair. The public key of the key pair must comply the regulations in section 6.1.5 Key Size and section 6.1.6 Public Key Parameter Generation and Quality Check and the private key may not be a weak key.

6.1.2 Private Keys Delivery to Subscriber

Not applicable

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber self-generates the key pair and transmits the certificate application file in PKCS# 10 format to the RA. The RA follows the regulations in section 3.2.1 Proof of Private Key Ownership. After checking that the subscriber has possession of the private key, the subscriber's public key is delivered to the GTLSCA by transport layer security protocol or another data encryption method having an equivalent security strength.

6.1.4 CA Public Key Delivery to Relying Parties

The GTLSCA public key certificate is issued by the eCA and published at the eCA and GTLSCA repositories for direct downloading and use by subscribers and relying parties.

6.1.5 Key Sizes

1. The GTLSCA uses RSA keys at least 2048 bits in size and SHA-256, SHA-384 or SHA-512 hash function to issue certificates.

2. Subscribers use RSA key at least 2048 bits in size.

6.1.6 Public Key Parameters Generation and Quality Checking

1. The public key parameter of the RSA algorithm is null.

2. The GTLSCA uses the ANSI X9.31 algorithm or FIPS 186-4 standard to generate the prime numbers needed for the RSA algorithm. This method can guarantee that the generated prime numbers are strong prime.

3. Subscribers use the software and hardware cryptographic module to generate the prime numbers for the RSA algorithm during the key generation process to ensure that the prime numbers are strong prime.

   According to NIST SP 800-89 section 5.3.3, the GTLSCA verifies that the value of the public exponent is greater than 3 odd numbers and this value is between $2^{16}+1$ and $2^{256}-1$. In addition, the modulus is an odd number, not a power of a prime and has no factors smaller than 752.

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

1. The GTLSCA signature-use private key may be only used for issuing certificate, CRL and OCSP response messages.

2. The GTLSCA's public certificate key usage extension is set to digitalSignature, keyCertSign and cRLSign.

3. SSL/TLS certificate key usage extension is set to digitalSignature and keyEncipherment. The extension key usage includes serverAuth and clientAuth.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The GTLSCA uses a hardware cryptographic module certified with FIPS 140-2 security level 3 authentication.

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

1. The GTLSCA's multi-person control of key splitting uses m-out-of-n method for the key split backup, initiation and recovery method.

2. After key generation, the GTLSCA splits the key into 5 parts and stores them is separate secure locations. At least three parts must be obtained to perform key recovery.

6.2.3 Private Key Escrow

1. The GTLSCA's signature-use private key cannot be escrowed.

2. The GTLSCA does not provide subscriber private key escrow.

6.2.4 Private Key Backup

The GTLSCA uses key splitting multi-person control methods to back up the private key and IC cards which have passed FIPS 140-2 security level 2 certification (or above) to act as the secret splitting storage media.

6.2.5 Private Key Archival

1. The GTLSCA's signature-use private key cannot be archived but the corresponding public key is archived in certificate file format in accordance with the regulations in section 5.5 Record Archiving Methods.

2. The GTLSCA does not archive the subscriber signature-use private key.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The GTLSCA transfers the private key into the cryptographic module under the following circumstances:

1. Key generation.

2. Key splitting backup recovery.

3. Cryptographic module replacement.

6.2.7 Private Key Storage on Cryptographic Module

1. Private keys are stored in cryptographic module in accordance with regulations.

2. If the cryptographic module does not need to be used, it must be taken offline and stored in a secure location.

6.2.8 Method of Activating Private Key

1. GTLSCA private key activation is controlled by multi-person control IC cards. IC card sets are kept by the administrator and officer.

2. The activation method for subscriber private key depends on the private key storage method type as described below:

   (1) Hardware cryptographic module: The activation method for private key must be controlled by a multi-person control IC card.

   (2) Other private key token: The subscriber shall use a high strength passcode or other equivalent level authentication methods to activate the private key.

6.2.9 Method of Deactivating Private Key

1. The GTLSCA's private key is deactivated using a multi-person control method.

2. The GTLSCA does not provide private key deactivation service to subscribers.

6.2.10 Method of Destroying Private Key

1. Destruction of GTLSCA private keys is performed as follows:

   (1) When the old private key is no longer being used, the GTLSCA performs zeroization of the memory address in the old private key stored in the hardware cryptographic module to destroy the old private key in the hardware cryptographic module. The corresponding key backup secret splitting IC card are also physically destroyed at this time.

   (2) When the hardware cryptographic module is replaced, all of the private key inside are destroyed. The key management

tool in the hardware cryptographic module is then used to verify that all of the private keys have been destroyed.

2. The destruction method for subscriber private key is not stipulated.

6.2.11 Cryptographic Module Rating

Cryptographic module rating is done in accordance with the regulations in section 6.2.1 Cryptographic Module Standards and Controls.

6.3 Other Aspects of Key Pair Management

The GTLSCA is not responsible for the safekeeping of subscriber private keys.

6.3.1 Public Key Archival

The GTLSCA shall perform certificate archiving work in accordance with the regulations in section 5.5 Record Archiving.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 PublicCA Certificate Operational Periods and Key Pair Usage Periods

1. The maximum usage period for GTLSCA public and private keys is 20 years.

2. The maximum usage period for private keys that issue subscriber certificates is 10 years.

3. After the private key that are used to issue subscriber certificates expires, the validity of the CRL or OCSP responder certificate must be continued until all of the subscriber certificates issued by the private key expire.

6.3.2.2 Subscriber Certificate Operational Periods and Key Pair Usage Periods

The validity of subscriber public certificates may not exceed 825 days as specified in the official version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

After being randomly generated by and written into the hardware cryptographic module, the GTLSCA private key activation data is then written into the m-out-of-n control IC card.

6.4.2 Activation Data Protection

1. The GTLSCA activation data is protected by the m-out-of-n control IC card and must be accessed through the hardware cryptographic module's built-in card reader. The IC card's individual's ID number is entered (PIN number) with the keyboard built-in the hardware cryptographic module.

2. The above IC card's PIN number may not be stored in any media.

3. If there are over three failed log-in attempts, the IC card is locked.

4. The personnel responsible for safekeeping must reset the PIN number during IC card handover.

6.4.3 Other Aspects of Activation Data

Not stipulated

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The GTLSCA provides the following security control functions:

1. Identity verification login.
2. Self-discretionary access controls.
3. Security audit capability.
4. Access control restrictions to certificate services and PKI trusted roles.
5. Identify and authenticate PKI trusted roles and related identities.
6. Ensure security of each communication and databases with password technology
7. Provide secure and reliable channels for PKI trusted roles and related identity verification.
8. Offer procedure integrity and security control protection.
9. Account numbers that have the right to issue certificates all should use multi-factor authentication methods to verify identity.

6.5.2 Computer Security Rating

The GTLSCA uses computer systems with security levels equivalent to C2(TCSEC), E2(ITSEC) or EAL3(CC) computer operating systems and its system and operating environment comply with WebTrust Principles and Criteria for Certification Authorities security control principles.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

1. Development and quality controls are implemented according to the software program development methods and quality management standards approved by competent authorities.
2. The system development environment, testing environment and official environment shall be operated separated in order to prevent unauthorized access or change.
3. Use of dedicated or authorized software and hardware.
4. Each product or program handed over to the GTLSCA must include a handover checklist, testing report and original program scanning report. Program version control is implemented and the software's original program code must be scanned regularly.

6.6.2 Security Management Controls

1. No unrelated software, hardware or components may be installed or operated.

2. Make sure the vendor has provided the complete and correct version of the software during software installation and automatically check the software integrity every day.

3. System configuration changes must be recorded and controlled.

4. Must have a modified system software or configuration detection mechanism.

6.6.3 Life Cycle Security Controls

At least one key compromise risk evaluation shall be conducted each year at the GTLSCA.

6.7 Network Security Controls

1. GTLSCA servers and its repository are isolated by security protection devices.

2. The repository is bulid in DMZ and connected to the Internet.

3. The repository prevents DDoS and intrusion attacks with system patch file updates and information security systems.

6.8 Time-stamping

The GTLSCA regularly conducts system synchronization with a reliable time source to ensure the accuracy of the following times and performs audits on the system synchronization work:

1. Subscriber certificate issuance times

2. Subscriber certificate revocation times

3. CRL issuance times

4. System event occurrence times

6.9 Cryptographic Modules Security Controls

Follow regulations in Section 6.1 Key Pair Generation and Installation and Section 6.2 Private Key Protection and Cryptographic Module Security Controls.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificates issued by the GTLSCA follow the current versions of ITU-T X.509, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by CA/Browser Forum, RFC 5280 or relevant regulations in their latest version.

The GTLSCA uses a cryptographically secure pseudorandom number generator (CSPRNG) to generate the serial numbers for issued certificates. These serial numbers are non-sequential positive integers at least 64 bits in size.

7.1.1 Version Number(s)

The GTLSCA issues X.509v3 version certificates in accordance with RFC5280 standards

7.1.2 Certificate Extensions

Certificate extensions follow the regulations in ITU-T X.509, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum, RFC 5280 and related technical specifications.

7.1.2.1 Subordinate CA Certificate of GTLSCA

GTLSCA certificate extension content is as follows:

Extension Name	Necessity	Criticality	Content
Authority Key Identifier	Necessary	FALSE	eCA public key SHA-1 hash value
Subject Key	Necessary	FALSE	GTLSCA public key SHA-1 hash

Extension Name	Necessity	Criticality	Content
Identifier			value
Certificate Policies	Necessary	FALSE	This extension shows the GTLSC has received eCA approval and are allowed to use the certificate policy object identifier number including: ■ PKI defined certificate object identifier number(Assurance Level 3). ■ CA/Browser Forum defined organization verification type SSL certificate policy object identifier number 「2.23.140.1.2.2」.
CRL Distribution Points	Necessary	FALSE	CARL download site posted by the eCA
Authority Information Access	Necessary	FALSE	This extension includes the following two information items: ■ eCA self-signed certificate download website ■ OCSP inquiry service website provided by the eCA
Basic Constraints	Necessary	TRUE	Subject Type=CA Path Length Constraint=0 (the GTLSCA no longer issues subordinate CA certificates downwards so the pathLenConstraint extension is set to 0)
Key Usage	Necessary	TRUE	keyCertSign, digitalSignature and cRLSign (in order to reserve the possibility of future use of the signature private key issuance of OCSP response messages by the GTLSCA, the key usage extension includes digitalSignature)
Name Constraints	Prohibited	TRUE	The GTLSCA does not use this extension
Extended Key	Necessary	FALSE	Server verification

Extension Name	Necessity	Criticality	Content
Usage			(1.3.6.1.5.5.7.3.1) Subscriber verification (1.3.6.1.5.5.7.3.2)

7.1.2.2 Subscriber Certificate

The subscriber certificate extension content is as follows:

Extension Name	Necessity	Criticality	Content
Authority Key Identifier	Necessary	FALSE	GTLSCA public key SHA-1 hash value
Subject Key Identifier	Necessary	FALSE	Subscriber public key SHA-1 hash value
Certificate Policies	Necessary	FALSE	This extension shows the certificate policy object identifier number used by GTLSCA which includes: ■ GTLSCA certificate policy object identifier number(Assurance Level 3). ■ CA/Browser Forum defined organization verification type SSL certificate policy object identifier number 「2.23.140.1.2.2」.
CRL Distribution Points	Necessary	FALSE	CRL download site posted by the GTLSC
Authority Information Access	Necessary	FALSE	This extension includes the following two information items: ■ GTLSCA CA certificate download site. ■ The OCSP inquiry service website provided by GTLSCA
Basic Constraints	Prohibited	FALSE	This extension is not used by the GTLSCA
Key Usage	Necessary	TRUE	digitalSignature and keyEncipherment

Extension Name	Necessity	Criticality	Content
Extended Key Usage	Necessary	TRUE	Server verification (1.3.6.1.5.5.7.3.1) Subscriber verification (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	Necessary	FALSE	Records the fully qualified domain names included on this SSL/TLS certificate.(This extension includes at least one FQDN)
Subject Directory Attributes	Necessary	FALSE	This extension includes the extra attributes of the SSL/TLS certificate type
Signed Certificate Timestamp List	Necessary	FALSE	Several certificate transparency log server reply signed certificate timestamp (SCT) are recorded in this extension

The GTLSC does not allow the issuance of certificates under the following two circumstances:

1. The certificate extension contains settings that cannot be used on a public network.
2. The certificate contains semantics that could mislead the relying parties to believe this certificate information has been verified by the GTLSCA.

The GTLSCA uses X.509 v3 extension methods to support certificate transparency (CT). The methods are as follows:

1. The GTLSCA transmits the unsigned precertificate as defined in RFC 6962 to several certificate transparency logs and waits for the individual reply SCT.

2. The time stamped signed certificates that meet quantity requirements are encapsulated into the X.509v3 extension of the pre-signed certificate and the pre-signed certificate is signed and encapsulated to complete certificate issuance.

3. Pre-signed certificates referred to in the aforementioned operations are only used for the certificate transparency X.509v3 extension method and may not be regarded as compliant with RFC 5280.

7.1.3 Algorithm Object Identifiers

The GTLSCA uses the following algorithm object identifiers:

Type	Algorithm	Algorithm Object Identifier
Signature	sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
	sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
Key generation	rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

The subject and issuer fields of the certificate must use the X.500 distinguished name and name attribute type shall comply with the current version of the ITU-T X.509, RFC5280 and Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum or related regulations in the latest versions. See section 3.1.5 for an explanation of certificate subject name fields.

7.1.4.1 Issuer Information

In accordance with RFC 5280 name changing regulations, the content of the issuer distinguished name in subscriber certificates issued by the GTLSCA must be identical to the content of the subject distinguished name in the GTLSCA's own certificates.

7.1.4.2 Subject Information–Subscriber Certificates

1. Only a verified fully qualified domain name that has passed through section 3.2.2.2 Domain Name Ownership Authentication Procedure may be recorded as the subscriber certificate subject name's common name field attribute and certificate subject extension.

2. If the subscriber certificate is a multi-domain SSL/TLS certificate, only one of the fully qualified domain names in the certificate subject alternative name extension may be recorded as the subscriber certificate subject name's common name field attribute.

3. 「.」,「-」or「 」(space) may not be the only characters recorded as the subscriber certificate subject field attribute. Also, no indication may be made that this value does not exist, is incomplete or not applicable.

4. The symbol 「_」 may not be included in the fully qualified domain name recorded in the subscriber certificate's certificate subject alternative name extension.

5. See the description in section 7.1.2.2 Subscriber Certificate for the subscriber certificate's certificate subject alternative name extension criticality and format.

6. Required / optional in the subscriber certificate subject distinguished name field explanation is as follows;

Subject Unique Identification Name Field	**Required / Optional**
subject:commonName (OID 2.5.4.3)	Optional
subject:organizationName (OID 2.5.4.10)	Required
subject:givenName (OID 2.5.4.42)	Prohibited
subject:surname (OID 2.5.4.4)	Prohibited
subject:streetAddress (OID 2.5.4.9)	Optional
subject:stateOrProvinceName (OID 2.5.4.8) or subject:localityName (OID 2.5.4.7)	Must include at least one item
subject:postalCode(OID 2.5.4.17)	Prohibited
subject:countryName(OID 2.5.4.6)	Required
subject:organizationUnitName(OID2.5.4.11)	Optional

7.1.4.3 Subject Information–CA Certificates

The GTLSCA's CA certificate subject distinguished name includes three attributes: commonName, organizationName and countryName.

1. commonName: Name that identifies the GTLSCA. This name is the certificate's unique identifier and can serve as a way to distinguish it from other certificates.

2. organizationName: The official organization name of the GTLSCA.

3. countryName: The country where the operation site of the GTLSCA is located. It is listed as "TW" in the ISO 3166-1 international standards.

7.1.5 Name Constraints

Certificates issued by the GTLSCA do not use nameConstraints.

7.1.6 Certificate Policy Object Identifier

Besides the certificate policy object identifier, the certificate policy extension includes the organization validation SSL certificate's certificate policy object identifier 「2.23.140.1.2.2」 defined by the CA/Browser Forum.

7.1.7 Usage of Policy Constraint Extension

Certificates issued by the GTLSCA do not contain policyConstraints.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by the GTLSCA do not contain policyQualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

For subscriber certificates issued by the GTLSCA, their critical certificate policy extension semantics must follow the regulations in the ITU-T X.509, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum and RFC 5280.

7.2 CRL Profile

7.2.1 Version Number(s)

The GTLSCA issues CRL that comply with ITU-T X.509 v2.

7.2.2 CRL and CRL Entry Extensions

crlExtensions and crlEntryExtensions must follow the regulations in the ITU-T X.509, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser

Forum, RFC 5280 and other latest versions.

7.3 OCSP Profile

1. The GTLSCA provides an OCSP inquiry service that complies with the RFC 6960 and RFC 5019 standards and includes the GTLSCA OCSP service website in the CA Access Information (AIA) extension of the certificate.

2. The OCSP inquiry packet for the GTLSCA OCSP inquiry service should include the following information:

   - Version number
   - Inquiry certificate identifier including: hash algorithm, CA issuer name, CA issuer public key and version number of the inquiry certificate.

3. The basic fields of the GTLSCA OCSP response message are as follows:

Field	Description
Version	v.1 (0x0)
OCSP responder ID	OCSP responder subject name
Produced time	Response message signature time
Inquiry certificate identifier	Includes hash algorithm, CA issuer name, CA issuer public key and version number of the inquiry certificate
Certificate status	Corresponding certificate status (0:Valid/1:Revoked/2:Unknown)
ThisUpdate/NextUpdate	Valid interval of recommended response packet including ThisUpdate and NextUpdate
Signature algorithm	Signature algorithm of response packet may be sha256WithRSAEncryption
Signature	OCSP responder signature
Certificates	OCSP responder certificates

7.3.1 Version Number(s)

Version numbers comply with RFC 5019 and RFC 6960 standards.

7.3.2 OCSP Extensions

1. OCSP extensions follow the regulations in ITU-T X.509, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA, RFC 5019 and RFC 6960.

2. OCSP response message extension include the OCSP certificate authority key identifier.

3. When the certificate status protocol inquiry packet includes a nonce field, the OCSP response message must include the same nonce field.

7.3.3 Regulations for Operation of OCSP

The GTLSCA OCSP inquiry service operation is comprised of the following:

1. Able to use the HTTP GET/POST method to process and accept the OCSP inquiry packet transmitted by OCSP subscribers.

2. The short-term certificate used the by OCSP responder are issued and updated by the GTLSCA.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

1. The GTLCSA conducts one internal audit each year.

2. The GTLCSA receives one external audit each year and audit period may not exceed 12 months.

3. The standards used for the audits are WebTrust Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

8.2 Identity/Qualifications of Assessor

1. Auditors must be authorized by WebTrust for CA seal management unit as auditors qualified to conduct audits compliant with WebTrust Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

2. Auditors must be qualified Certified Information Systems Auditor(CISA) or have the same level qualifications.

3. The GTLCSA shall verify the identities of the audit personnel during the audit.

8.3 Assessor’s Relationship to Assessed Entity

Auditors shall be independent of audited certification administration authority and be an independent and impartial third party.

8.4 Topics Covered by Assessment

1. Whether GTLSCA CPS complies with eCA CP and CPS regulations.

2. Whether the GTLSC and RA comply with GTLSCA CPS operations.

3. The GTLSC must follow the latest version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum and randomly sample at least 3% (randomly sample one if less than one) each quarter for verification.

8.5 Actions Taken as a Result of Deficiency

1. The GTLSCA make improvements of the non-compliances and notify the original auditor after completion to conduct a re-audit.

2. The GTLSCA shall take whatever measures that are necessary depending on the type of non-compliance, severity and time needed to make the corrections.

8.6 Communications of Results

1. Except for those circumstances which could result in system security risks and the stipulations in section 9.3 Confidentiality of Business Information, the GTLSCA shall publish the most recent external audit report and management statement at the repository within three months after the audited area is completed. If there is a delay in publication, the letter of explanation should be provided to the qualified auditor.

2. The audit results are displayed on the front page of the GTLSCA website in accordance with WebTrust Principles and Criteria for Certification Authorities and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security seal regulations. The external audit report and management statement can be read by clicking on the seal.

3. The contents of the disclosed audit document must comply with related browser trust root certificate programs.

9 Other Business and Legal Matters

9.1 Fees

No fees are being collected at this time.

9.1.1 Certificate Issuance or Renewal Fees

No fees are being collected at this time.

9.1.2 Certificate Access Fees

No fees are being collected at this time.

9.1.3 Revocation or Status Information Access Fees

No fees are being collected at this time.

9.1.4 Fees for Other Services

No fees are being collected at this time.

9.1.5 Refund Policy

No fees are being collected at this time.

9.2 Financial Responsibility

GTLSCA operations are maintained with funding budgeted by the government. No insurance policies have been taken out with insurance companies. Other related financial obligations are handled in accordance with related laws and regulations.

9.2.1 Insurance Coverage

Not applicable

9.2.2 Other Assets

Not applicable

9.2.3 Insurance or Warranty Coverage for End Entities

Not applicable

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

1. Private key and passwords for GTLSCA operation.
2. Related GTLSCA key splitting information.
3. Subscriber information not authorized for disclosure
4. Records produced or kept by the GTLSCA for audit or tracking purposes.
5. Audit logs and findings generated by auditors during the audit process which may not be fully disclosed
6. Operation-related documents designated as non-disclosable by the GTLSCA.
7. Other non-disclosable information as stipulated by law.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not specified in section 9.3.1 Scope of Sensitive Information is considered to be, in principle, non-sensitive information.

9.3.3 Responsibility to Protect Confidential Information

The GTLSCA follows the regulations in the Electronic Digital Signature Act, WebTrust Principles and Criteria for Certification Authorities、WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum and the Personal Information Protection Act when processing sensitive GTLSCA information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

1. The privacy protection policy is published on the GTLSCA website.
2. The GTLSCA implements privacy impact analysis and personal information risk assessment measures.

9.4.2 Information Treated as Private

1. Personal information listed on the certificate application.
2. Personal information obtained during GTLSCA operations.

9.4.3 Information Not Deemed Private

Any information not specified in section 9.4.2 Types of Private Information is considered to be, in principle, non-sensitive information.

9.4.4 Responsibility to Protect Private Information

The Private Rights Protection Policy, WebTrust Service Principles and

Criteria for Certification Authorities, WebTrust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum and the Personal Information Protection Act regulations published at the website are followed to protect private information.

9.4.5 Notice and Consent to Use Private Information

1. The privacy right protection policy is published on the website.
2. Subscriber consent must be obtained before private personal information is used.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

If sensitive information must be accessed by judicial or law enforcement authorities for investigative or evidence collection purposes, the GTLSCA shall follow relevant legal procedures. No additional notification will be provided to the subscriber.

9.4.7 Other Information Disclosure Circumstances

Relevant legal procedures are followed.

9.5 Intellectual Property Rights

Except for personal information, the documents (including electronic files) generated by the GTLSCA and its intellectual property are the property of the GTLSCA. Reproduction and dissemination must be handled in accordance with the regulations in the copyright statement published at the website.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

1. Conduct operations in accordance with CP assurance level 3 regulations and GTLSCA CPS.
2. Implement certification application identification and authentication procedures.
3. Issuance, publication and revocation of certifications.
4. Issuance and publication of CRL.
5. Provisions of OCSP inquiry services.
6. Generation and management of GTLSCA private keys.

9.6.2 RA Representations and Warranties

1. Provision of certificate application services.
2. Implementation of certificate application identification and authentication procedures.
3. Management of RA private keys and prohibition of use outside of certificate registration.

9.6.3 Subscriber Representations and Warranties

1. Provisions of accurate and complete information.
2. Compliance with GTLSCA CPS regulations.
3. Proper safekeeping and use of private keys.

4. The GTLSCA shall be notified immediately to revoke the certificate in the event of private key spoofing, compromise or loss. However, legal liability for use of the certification prior to the change must be borne by the subscriber.

5. Secure generation of the private key and take precautions to prevent compromise.

6. The subscriber shall prudently select a secure computer environment and trustworthy application system. In the event that relying parties suffer damages due to computer environment or application system factors, the subscriber shall bear sole liability.

7. In the event that normal services cannot be provided by the GTLSCA, the subscriber shall promptly seek out other means to fulfill their obligations to other parties and not use GTLSCA's inability to provide services as a defense to other parties.

9.6.4 Relying Parties Representations and Warranties

1. Comply with GTLSCA CPS regulations.

2. Check accuracy of the certificate digital signature, validity and key usage.

3. Relying parties shall ensure the security of the certificate use environment. Relying parties shall bear sole liability when rights and interests are infringed due to reasons not attributable to the GTLSCA.

4. In the event that normal services cannot be provided by the GTLSCA, the subscriber shall promptly seek out other means to

fulfill their obligations to other parties and not use GTLSCA's inability to provide services as a defense to other parties.

9.6.5 Representations and Warranties of Other Participants

As appointed by the NDC, the GTLSCA handles contracted services in accordance with the regulations in the Government Procurement Act. The contractors follow relevant contract provisions.

9.7 Disclaimer of Warranties

The subscriber or relying party shall be solely liable for damages resulting from the failure of the subscriber or relying party to follow certificate application, management and use regulations which are unavoidable or not attributable to the GTLSCA. The GTLSCA shall bear no legal liability.

9.8 Limitations of Liability

1. If some certificate services must be suspended due to GTLSCA maintenance, conversion or expansion requirements, notification shall be posted at the repository three days in advance. Subscribers and relying parties may not use this as a reason to claim compensation from the GTLSCA.

2. The GTLSCA shall issue and manage SSL/TLS certificates in accordance with the regulations in the formal version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum.

3. If the subscriber needs to revoke the certificate, a certificate revocation application is submitted in accordance with Certificate Suspension and Revocation regulations. After the

certificate revocation application is approved, the GTLSCA completes the certificate revocation work within one working day and issues and publishes the CRL at the repository.

4. Before the certificate revocation status is published, the subscriber shall take appropriate action to mitigate the effect on relying parties and bear all liability from use of the certificate.

9.9 Indemnities

9.9.1 Indemnification by GTLSCA

In the event that a stakeholder is impaired due to GTLSC failure to comply with the GTLSCA CPS or relevant laws and regulations, the GTLSC shall be liable for indemnity, and the subscriber and relying party may request indemnity for damages in accordance with the law.

9.9.2 Indemnification by RA

In the event that a stakeholder is impaired due to RA failure to comply with the GTLSCA CPS or relevant laws and regulations, the RA shall be liable for indemnity, and the subscriber and relying party may request indemnity for damages in accordance with the law

9.10 Term and Termination

9.10.1 Term

GTLSCA CPS takes effect after approval and announcement by the GTLSC. It remains valid until it is replaced by the most recent version.

9.10.2 Termination

Termination of the GTLSCA CPS must be resolved by the NDC and

approved the GTLSCA.

9.10.3 Effect of Termination and Survival

1. Information on GTLSCA CPS validity and termination shall be announced at the GTLSC repository.

2. After GTLSCA CPS termination, it shall remain validity until the last issued certificate expires.

9.11 Individual Notices and Communications with Participants

The GTLSCA, RA, subscribers and relying parties shall establish notification and communication channels by website notification, repository, official document, letter, telephone, fax and email.

9.12 Amendments

The GTLSC performs a regular annual review of the provisions of the official version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum to determine whether the GTLSC CPS needs to be amended. In the event that the SSL/TLS issuance and management regulations in the GTLSC CPS conflict with the forum regulations, the regulations issued by the CA/Browser shall prevail and the GTLSCA CPS shall be modified accordingly. The amended version shall be implemented following approval by the GTLSC. The amendment method is as follows:

1. Direct amendment of the GTLSCA CPS content.

2. Amendment done by attached document.

9.12.1 Procedure for Amendment

Amendments to the GTLSCA CPS are reviewed by the NDC and announced following approval by the GTLSC.

9.12.2 Notification Mechanism and Period

9.12.2.1 Notification Mechanism

All modified items are published at the repository.

9.12.2.2 Modified Items

The publishing period of draft version is at the repository following NDC review is determined based on what level of impact the modifications have on subscribers or relying parties. The notification period is as follows:

1. Significant impact: Published at the repository for 15 calendar days before submission to the GTLSCA for examination.

2. Less significant impact: Published at the repository for 7 days before submission to the GTLSCA for examination.

No addition notification is given for new layouts, glossary changes and word error corrections.

9.12.2.3 Comment Reply Period

The reply period for subscriber and relying party comments about modifications is as follows:

1. Significant impact: The reply period is within 15 calendar days of the posting date.

2. Less significant impact: The reply period is within 7 days of the posting date.

9.12.2.4 Comment Processing Mechanism

1. Comments made about modifications before the end of the reply period shall be submitted by email to the GTLSCA.

2. The GTLSC shall reply to the comments following evaluation.

9.12.2.5 Final Notification Period

GTLSCA CPS amendments must be announced within 10 calendar days following approval by the GTLSC.

9.12.3 Circumstances under which OID Must Be Changed

If the CP is amended or the OID is changed, the GTLSCA CPS shall also be amended accordingly.

9.13 Dispute Resolution Provisions

In the event of a dispute between a subscriber and the GTLSCA, the parties shall first conduct negotiations in good faith and explanations of relevant regulations in the GTLSCA CPS shall be provided by the GTLSCA.

9.14 Governing Law

Related ROC laws and regulations shall govern.

9.15 Compliance with Applicable Law

Related ROC laws and regulations shall apply. ◦

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This GTLSCA CPS constitutes the final and entire agreement between the key participants (GTLSCA, RA, subscribers and relying parties) and supersedes all prior oral or written understandings relating to the same subject matter and this GTLSCA CPS represents the final agreement.

9.16.2 Assignment

The rights and obligations of the key participants outlined in the GTLSCA CPS may not be assigned in any form to other parties without notifying the GTLSCA.

9.16.3 Severability

1. If any chapter of the CPS is found to be not applicable, the remaining chapters of the CPS shall remain valid

2. The GTLSCA follows the regulations in the official version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum. However, if relevant regulations are in conflict with ROC law and regulations, the GTLSCA may make minor adjustments to related methods to satisfy legal or regulatory requirements and notify the CA/Browser Forum about the modified sections before issuing new certificates. Under the following circumstances, the deleted or modified content of the original CPS shall need to pass NDC review and receive GTLSCA approval. The above work must be completed within 90 days.

(1) The related regulations in the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum that are in conflict with ROC laws and regulations have be modified or eliminated.

(2) The CA/Browser Forum has modified the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates regulations and the modifications are compatible for ROC laws and regulations.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

1. In the event that the GTLSCA suffers damages attributable to an intentional or unintentional violation or related GTLSCA CPS regulations by a subscriber or relying party, the GTLSCA may, besides seeking compensation for damages, request the responsible party to pay the attorney fees arising from handling this dispute or litigation.

2. The GTLSCA's failure to assert rights regarding the violation of GTLSCA CPS regulations does not forfeit the GTLSCA's right to pursue violations of GTLSCA CPS regulations.

9.16.5 Force Majeure

In the event that damages are incurred due to a force majeure or other reasons not attributable to the GTLSCA, the GTLSCA shall bear no legal liability.

9.17 Other Provisions

Not stipulated

Appendix 1: Glossary

◆ A

- **Activation Data:** Except for keys, the private data required to access the cryptographic module (such as data used to activate the private key for signatures or encryption).

- **Applicant**: A subscriber who has requested a certificate from a CA but has not yet completed the certificate procedure.

- **Archive**: A physically separate storage site for long-term information (storage site for key information) which can be used to support audit, availability and integrity services.

- **Assurance:** A basis that the trusted entity has complied with to certain security requirements.

- **Assurance Level**: A certain level in a relative assurance tier.

- **Audit:** Assessment of whether system controls are adequate to ensure conformity with existing policy and operation procedures, and independent checking and review of recommended required improvements to existing controls, policies and procedures

- **Audit Log:** Activity logs of a system arranged in the order of time of occurrence that can be used to reconstruct or investigate the time sequence or changes that occurred during a certain event.

- **Authenticate:** Authenticating is a process by which a claimed

identity is determined to be legitimate and belonging to the claimant.

- **Authentication**
  - The process of establishing a level of trust in the identity of subscribers or information systems.
  - Security measures used for information transmission, messages, and methods to authorize individuals to receive certain types of information.

◆ **C**

- **Certificate**
  - Refers to verification information carrying a digital signature used to verify the identity and qualifications of the signer in electronic form
  - Digital presentation of information. The contents include:
    - ✓ Issuing certificate authority
    - ✓ Subscriber name or identity
    - ✓ Subscriber public key
    - ✓ Certificate validity period
    - ✓ Certificate authority digital signature

- **Certificate Policy (CP)**： Refers to the dedicated profile administration policy established for the electronic transactions performed through the certificate administration. Certificate policy covers a variety of issues including the formation, generation, delivery, auditing, auditing, restoration after compromise and administration. The security services required for a certain application are provided through certificate policy

and other related technology

- **Certificate Problem Report:** Reporting of suspected key compromise or certificate misuse, counterfeiting, compromise or abuse complaints.

- **Certificate Revocation List (CRL)**
  - The revoked certificate list digitally signed by the certificate authority provided for relying party use.
  - List maintained by the certificate authority. The expiry dates of the above revoked certificates issued by the certificate authority are recorded on the list.

- **Certification Authority (CA)**
  - The certificate issuance entity.
  - The competent body trusted by the subscriber. Its functions are the issuance and administration of X.509 format public key certificates, CARLs and CRLs.

- **Certification Authority Authorization (CAA)**: According to RFC 6844 regulations, the Certification Authority DNS Resource Record permits a domain name owner in the DNS to designate one or more CAs to obtain authorization to help that domain with certification issuance. Publication of the CAA resource record allows publicly trusted CAs to implement extra controls to reduce unforeseen certificate mis-issuance risk.

- **Certificate Modification:** Refers to providing a new certificate to replace the original certificate to the same certificate subject. However, the expiry date of the new certificate must be the same

as that on the old certificate. The old certificate is revoked after certificate modification

- **Certification Practice Statement (CPS)**
  - External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work.
  - Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, extension and access) comply with certain requirements (these requirements are described in the certificate policy or other service contracts).

- **Certificate Transparency (CT)**: An open source framework for the public monitoring and auditing of all certificates on the Internet (TLS/SSL certificate are currently the priority target). By giving public certificate issuance and existence information to domain owners, CA and domain users, it can be determined whether the certificate has been mistakenly or maliciously issued. In other words, its purpose is to provide an open environment which can be used to monitor the TLS/SSL certificate mechanism and review the open monitoring of certain TLS/SSL certificates and their information to reduce related certificate threats. The CT mechanism is primarily comprised of transparency logs, certificate monitors and certificate auditors.

- **Common Criteria for Information Technology Security Evaluation:** Abbreviated as Common Criteria or CC. An information security product evaluation and verification standard

developed by the governments of Canada, France, Germany, the UK, and the U.S. that was formally made into an ISO standard (ISO/IEC 15408) in August 1999. The standard is used to evaluate whether the product can receive an Evaluation Assurance Level (EAL) which describes the depth and rigor of the product security standard testing. There are seven EAL with EAL1 being the lowest level and EAL7 being the highest level. At present, only the highest-level IT product security certification performed by a third-party testing laboratory accredited by multiple countries can be used a basis for purchasing and use of information product users.

- **Compromise**: Information disclosure to unauthorized persons or violation of information security policy which leads to the intentional or unintentional unauthorized disclosure, modification, destruction or loss of information

- **Cross-Certificate:** A certificate used to establish a trust relationship between two root certificate authorities. This certificate is a type of CA certificate and not a subscriber certificate.

- **Cryptographic Module**: A set of hardware, software, firmware or a combination of the above used to run cryptologic or programs (including crypto algorithms) and included within the cryptographic boundaries of the module.

- **Cryptographically Secure Pseudorandom Number Generator (CSPRNG)**: Random number generator for the encryption system.

◆ D

- **Digital Signature:** A digital signature is made up of digital information of a certain size calculated by mathematical algorithm or other methods that is encrypted with a signer's private key and may be verified with a public key.

- **Duration**: A certificate field made up of two subfields "start time of the validity period" and "end time of the validity period".

◆ E

- **End Entity (EE)**: The GPKI is comprised of the following two types of entities:
  - Those responsible for the safekeeping and use of certificate private keys.
  - Third parties who trust the certificates issued by the trusted CA (not holders of private keys and not a certificate authority). The end entities are subscribers and relying parties including persons, organizations, accounts, devices and sites.

- **ePKI Root Certification Authority:** The root certificate authority for the ePKI. It is the top certificate authority in the public infrastructure hierarchy. Its public key is a trust anchor.

◆ F

- **Federal Information Processing Standard (FIPS)**: Except for military organizations in the US federal government system, the information processing standard for all government organizations and government subcontractors. The security requirement

standard for the cryptographic module is FIPS no. 140 standard (FIPS 140). FIPS 140-2 divides the cryptographic module into 11 types of security requirements. Each security requirement type is then divided into 4 security levels.

- **Fully Qualified Domain Name (FQDN)**: A type of domain name that specifies the exact location of a specific computer in the domain hierarchy. The FQDN consists of two parts: the hostname (service name) and domain name and the hostname must be places at the starting place of the name. Here are some examples:

  - ourserver.ourdomain.com.tw：ourserver is the hostname, ourdomain.com.tw is the website name. Of these, ourdomain is a third level domain name, com is the subdomain name and tw is the country code top-level domain (ccTLD).
  - www.ourdomain.com: www is the hostname, ourdomain is the subdomain name and com is the generic top-level domain (gTLD).

◆ **I**

- **Information Technology Security Evaluation Criteria (ITSEC)**: A set of criteria for evaluating security that was first published in France, Germany, the Netherlands and the UK in 1991. The ITSEC defines seven security evaluation levels from E0 to E6. Different from the criteria to evaluate the trustworthiness of computer system security, it only describes technical security requirements and confidentiality is the security strengthening function. The importance of confidentiality, integrity and availability towards information security is

emphasized.

- **Internet Engineering Task Force (IETF):** Responsible for the development and promotion of Internet standards. Its vision of the generation of high-quality technical documents affects how persons design, use and manage the Internet and allows the Internet to operate smoothly. (official website: https://www.ietf.org)

- **Issuing CA:** For a particular certificate, the CA that issues the certificate is called the issuing CA.

-

◆ **K**

- **Key Escrow**: Storage of related information using the subscriber's private key and according to the terms of the escrow agreement (or similar contract). The terms of this escrow agreement require that one or more agencies are in possession of the subscriber key provided it is beneficial to the subscriber, employer or another party in accordance with the provisions of the agreement.

- **Key Pair:** Two mathematically linked keys possessing the following attributes:
  - One of the keys is used for encryption. This encrypted data may only be decrypted by the other key.
  - It is impossible to differentiate one key from another (from a mathematical calculation standpoint).

◆ **O**

- **Object Identifier (OID)**
  - One type of unique alphanumeric / numeric identifier registered under the International Standard Organization registration standard which could be used to identify the uniquely corresponding certificate policy.
  - When a special form of code, object or object type is registered with the International Organization for Standardization (ISO), the unique code can be used as an identifier. For example, this code can be used in the public key infrastructure to indicate which certificate policy and cryptographic algorithms are used.

- **Online Certificate Status Protocol (OCSP)**: The Online Certificate Status Protocol is a type of online certificate checking protocol which allows the application software of relying parties to determine the status (such as revoked or valid) of a certain certificate.

- **Online Certificate Status Protocol Responder (OCSP Responder)**: An online server authorized by the GCA. It is connected to the repository to process certificate status inquiry requests.

- **OCSP Stapling**
  - A type of TLS/SSL certificate status request extension that can be used in place of OCSP to become a type of X.509 certificate status checking method. Its operation mechanism is

as follows:

- ✓ The website obtains a time constraint OCSP response message from the OCSP responder and saves its temporarily.
- ✓ During each initial TLS connection process, the website transmits the temporarily saved OCSP response message to the subscriber (it is generally a browser). The subscriber only needs to verify that the response message is valid and does not have to send an OCSP inquiry packet to the CA.

■ The mechanism uses retransmission of the TLS/SSL certificate validity message routinely sent out by the OCSP responder to reduce the frequency of TLS/SSL certificate status inquiry made by the subscriber which lessens the burden on the CA.

- **Organization Validation (OV)**: In the SSL certificate approval process, except for identification and authentication of subscriber domain name control rights, following the certificate assurance level to identify and authenticate the identity of subscriber organizations and individuals. Therefore, a connection to a website established by an Organization Validation SSL certificate is able to provide TLS encryption channels, in order to determine who the owner of the website is and ensure the integrity of the transferred information.

◆ **P**

- **Private Key:** The following keys must be kept secret under these

two circumstances:

- It is the key in the signature key pair used to generate digital signatures.
- It is the key in the encryption key pair used for decrypt sensitive information.

- **Public Key:** The following keys must be made public (usually in digital certificate form) under these two circumstances:
  - It is the key in the signature key pair used to verify the validity of the digital signature.
  - It is the key in the encryption key pair used for encrypting sensitive information.

- **Public Key Infrastructure (PKI):** A combination of laws, policies, standards, personnel, equipment, technology, processes, audits and services developed on a broad scale and management of asymmetric cryptography and public key certificates.

Q

- **Qualified Auditor:** Complies with the qualification requirements in section 8.2 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser Forum and is an accounting firm, legal person or individual independent of the auditee.

R

- **Registration Authority (RA)**
  - Responsible for checking the identity and other attributes of

the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement.

- The entity responsible for the identity verification and authentication of the certificate subject which does not issue certificates.

- **Re-key (a Certificate)**: Rekeying a certificate refers to the issuance of a new certificate that has the same attributes and assurance level as the old certificate. In addition to being a brand-new certificate with a different public key (corresponding to the new and different private key) and different serial number, the new certificate may also be assigned a different validity period.

- **Relying Party**
  - Recipient of a certificate who relies on that certificate or a digital signature to verify the public key listed on the certificate or the counterpart to identify (or its attributes) the subject named in a trusted certificate and public key listed in the certificate.
  - The individual or agency which receives information including a certificate and digital signature (the public key listed on the certificate may be used to verify the digital signature) and that may rely on this information.

- **Renew a Certificate:** Refers to the issuance of a new certificate that has the same subject name, key and related information as

the old certificate to extend the validity period of the certificate and provide a new serial number.

- **Repository**
  - A trustworthy system used to store and retrieve certificates and other information relevant to certification.
  - The database containing the certificate policy and certificate-related information.

- **Revoke a Certificate:** Termination of certificate operation during its validity period.

- **Root Certification Authority (Root CA):** The highest-level CA in the GPKI. In addition to issuing subordinate CA certificates and self-signed certificates, application software providers are responsible for the distribution of its self-signed certificates. Can be called certificate root CA or top-level CA.

◆ **S**

- **Self-Signed Certificate:** Self-signed certificates are a type of certificate whose certificate issuer name is the same as the certificate subject name. Even if the private key from the same key pair is used to issue certificates with its corresponding public key and other information, a self-signed certificate inside the PKI can serve as a trust anchors for certificate path. Its issuance counterpart is the GTLSCA itself, Self-signed certificates contain the GTLSCA public key and the certificate issuer name and certificate subject name are the same. They are provided to relying parties for GTLSCA issued self-issued certificate,

subordinate CA certificate and CARL digital signature use.

- **Subordinate Certification Authority**: A certificate that is issued from another CA in the PKI hierarchy. Its actions are restricted to serving as a CA for another CA.

- **Subscriber**
  - Refers to a subject named or identified in the certificate that holds the private key that corresponds with the public key listed in the certificate.
  - An entity possessing the following attributes including (but not limited to) individuals, organizations and network devices:
    - ✓ Subject listed on an issued certificate
    - ✓ A private key that corresponds to the public key listed on the certificate
    - ✓ Other parties that do not issued certificates

- **Secure Socket Layer (SSL)**: Designed by Netscape, the SSL is primarily a secure protocol for sending information over the Internet. Internet communications can be encrypted at the transport layer to ensure the integrity of transmitted information. The identity of servers and subscribers can also be verified. This secure communication protocol can used before application layer communication to complete encryption calculation, communication key arrangement and server verification work. The most recent version is SSL 3.0. Google found design flaws in October 2014 and recommended its use be discontinued. Now, most have switched over to version TLS 1.3 secure communications protocol.

◆ T

- **Transport Layer Security (TLS)**: A type of secure communication protocol. In 1999, the IETF standardized the SSL and announced the first version of the TLS standard (RFC 2246) which was followed by the announcement of later versions: RFC 4346, RFC 5246 and RFC 6176 explaining TLS 1.1 and TLS 1.2. At present, the latest version announced by the IETF in 2019 is RFC 8446 which is TLS 1.3. It has removed many outdated and insecure functions (including MD5 and SHA-224 encryption functions) and added support for ChaCha20, Poly1305, Ed25519, Ed448, x25519 and x448. Support is also provided for 1-RTT and 0-RTT to reduce the delay time in connections between servers and subscribers.
- **Trusted Computer System Evaluation Criteria (TCSEC)**: The first formal standard for computer system evaluations. Proposed by the U.S. National Defense Science Council in 1970 and issued by the U.S. Department of Defense in 1985, the TCSEC divided computer system security into four 4 divisions and 7 security levels. Its primary emphasis is on operating system security. No emphasis is placed on system integrity.
- **Trustworthy System:** Computer hardware, software or programs which possess the following attributes:
  - Functions that protect against intrusion and misuse
  - Provides reasonably available, reliable and accurate operations
  - Appropriate execution of the preset function
  - Security procedures are uniformly accepted by the general public

◆ Z

- **Zeroization:** Method to delete electronically stored information. Storage of modified information to prevent recovery of information

Appendix 2: English Acronyms

Acronym	Full Name
AIA	Authority Info Access
CA	Certification Authority
CAA	Certification Authority Authorization
CC	Common Criteria for Information Technology Security Evaluation
CP	Certificate Policy
CP OID	Certificate Policy Object Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
DN	Distinguished Name
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IETF	Internet Engineering Task Force
ITSEC	Information Technology Security Evaluation Criteria
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validation
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority

Acronym	Full Name
RFC	Request for Comments
SSL	Security Socket Layer
TCSEC	Trusted Computer System Evaluation Criteria
TLS	Transport Layer Security

Appendix 3: BRs-Section 1.2.1 Revisions

The version of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates issued by the CA/Browser referred to by the initial version of the GTLSCA CPS is version 1.6.5.

Ver.	Ballot	Description	Adopted	Effective*	Implementation
1.0.0	62	Version 1.0 of the Baseline Requirements Adopted	22-Nov-11	01-Jul-12	—
1.0.1	71	Revised Auditor Qualifications	08-May-12	01-Jan-13	Compliant
1.0.2	75	Non-critical Name Constraints allowed as exception to RFC 5280	08-Jun-12	08-Jun-12	Compliant
1.0.3	78	Revised Domain/IP Address Validation, High Risk Requests, and Data Sources	22-Jun-12	22-Jun-12	Compliant
1.0.4	80	OCSP responses for non-issued certificates	02-Aug-12	01-Feb-13 01-Aug-13	Completed
--	83	Network and Certificate System Security Requirements adopted	03-Aug-13	01-Jan-13	Compliant
1.0.5	88	User-assigned country code of XX allowed	12-Sep-12	12-Sep-12	Compliant
1.1.0	--	Published as Version 1.1 with no changes from 1.0.5	14-Sep-12	14-Sep-12	—
1.1.1	93	Reasons for Revocation and Public Key Parameter checking	07-Nov-12	07-Nov-12	Compliant
1.1.2	96	Wildcard certificates and new gTLDs	20-Feb-13	20-Feb-13 01-Sep-13	Compliant
1.1.3	97	Prevention of Unknown Certificate Contents	21-Feb-13	21-Feb-13	Compliant
1.1.4	99	Add DSA Keys (BR v.1.1.4)	3-May-2013	3-May-2013	Compliant
1.1.5	102	Revision to subject domainComponent language in section 9.2.3	31-May-2013	31-May-2013	Compliant
1.1.6	105	Technical Constraints for Subordinate Certificate Authorities	29-July-2013	29-July-2013	Compliant
1.1.7	112	Replace Definition of “Internal Server Name” with “Internal Name”	3-April-2014	3-April-2014	Compliant
1.1.8	120	Affiliate Authority to Verify Domain	5-June-2014	5-June-2014	Compliant
1.1.9	129	Clarification of PSL	4-Aug-2014	4-Aug-2014	Compliant

		mentioned in Section 11.1.3			
1.2.0	125	CAA Records	14-Oct-2014	15-Apr-2015	Compliant
1.2.1	118	SHA-1 Sunset	16-Oct-2014	16-Jan-2015 1-Jan-2016 1-Jan-2017	Compliant
1.2.2	134	Application of RFC 5280 to Pre-certificates	16-Oct-2014	16-Oct-2014	Compliant
1.2.3	135	ETSI Auditor Qualifications	16-Oct-2014	16-Oct-2014	—
1.2.4	144	Validation Rules for .onion Names	18-Feb-2015	18-Feb-2015	Compliant
1.2.5	148	Issuer Field Correction	2-April-2015	2-April-2015	Compliant
1.3.0	146	Convert Baseline Requirements to RFC 3647 Framework	16-Apr-2015	16-Apr-2015	—
1.3.1	151	Addition of Optional OIDs for Indicating Level of Validation	28-Sep-2015	28-Sep-2015	Compliant
1.3.2	156	Amend Sections 1 and 2 of Baseline Requirements	3-Dec-2015	3-Dec-2016	Compliant
1.3.3	160	Amend Section 4 of Baseline Requirements	4-Feb-2016	4-Feb-2016	Compliant
1.3.4	162	Sunset of Exceptions	15-Mar-2016	15-Mar-2016	Compliant
1.3.5	168	Baseline Requirements Corrections (Revised)	10-May-2016	10-May-2016	Compliant
1.3.6	171	Updating ETSI Standards in CABF documents	1-July-2016	1-July-2016	—
1.3.7	164	Certificate Serial Number Entropy	8-July-2016	30-Sep-2016	Compliant
1.3.8	169	Revised Validation Requirements	5-Aug-2016	1-Mar-2017	Compliant
1.3.9	174	Reform of Requirements Relating to Conflicts with Local Law	29-Aug-2016	27-Nov-2016	Compliant
1.4.0	173	Removal of requirement to cease use of public key due to incorrect info	28-July-2016	11-Sep-2016	Compliant
1.4.1	175	Addition of givenName and surname	7-Sept-2016	7-Sept-2016	Compliant
1.4.2	181	Removal of some validation methods listed in section 3.2.2.4	7-Jan-2017	7-Jan-2017	Compliant
1.4.3	187	Make CAA Checking Mandatory	8-Mar-2017	8-Sep-2017	Compliant
1.4.4	193	825-day Certificate Lifetimes	17-Mar-2017	1-Mar-2018	Compliant
1.4.5	189	Amend Section 6.1.7 of Baseline Requirements	14-Apr-2017	14-May-2017	Compliant
1.4.6	195	CAA Fixup	17-Apr-2017	18-May-2017	Compliant

1.4.7	196	Define “Audit Period”	17-Apr-2017	18-May-2017	—
1.4.8	199	Require commonName in Root and Intermediate Certificates 9	9-May-2017	8-June-2017	Compliant
1.4.9	204	Forbid DTPs from doing Domain/IP Ownership	11-July-2017	11-Aug-2017	Compliant
1.5.0	212	Canonicalise formal name of the Baseline Requirements	1-Sept-2017	1-Oct-2017	Compliant
1.5.1	197	Effective Date of Ballot 193 Provisions	1-May-2017	2-June-2017	Compliant
1.5.2	190	Add Validation Methods with Minor Corrections	19-Sept-2017	19-Oct-2017	Compliant
1.5.3	214	CAA Discovery CNAME Errata	27-Sept-2017	27-Oct-2017	Compliant
1.5.4	215	Fix Ballot 190 Errata	4-Oct-2017	5-Nov-2017	Compliant
1.5.5	217	Sunset RFC 2527	21-Dec-2017	20-Jan-2018	Compliant
1.5.6	218	Remove validation methods #1 and #5	5-Feb-2018	9-Mar-2018	Compliant
1.5.7	220	Minor Cleanups (Spring 2018)	30-Mar-2018	29-Apr-2018	Compliant
1.5.8	219	Clarify handling of CAA Record Sets with no "issue"/"issuewild" property tag	10-Apr-2018	10-May-2018	Compliant
1.5.9	223	Update BR Section 8.4 for CA audit criteria	15-May-2018	14-June-2018	Compliant
1.6.0	224	WhoIs and RDAP	22-May-2018	22-June-2018	Compliant
1.6.1	SC6	Revocation Timeline Extension	14-Sep-2018	14-Oct-2018	Compliant
1.6.2	SC12	Sunset of Underscores in dNSNames	9-Nov-2018	10-Dec-2018	Compliant
1.6.3	SC13	CAA Contact Property and Associated E-mail Validation Methods	25-Dec-2018	1-Feb-2019	Compliant
1.6.4	SC14	Updated Phone Validation Methods	31-Jan-20	31-Jan-20	Compliant
	SC15	Remove Validation Method Number 9	5-Feb-2019		
	SC7	Update IP Address Validation Methods	8-Feb-2019		
1.6.5	SC16	Other Subject Attributes	15-Mar-2019	16-April-2019	Compliant

* Effective Date and Additionally Relevant Compliance Date(s)