Government TLS Certification Authority Certification Practice Statement Version 1.0.6

Administrative Organization: Ministry of Digital Affairs

Executive Organization: Chunghwa Telecom Co., Ltd
September 23, 2025

Version Revision Log

Version	Effective Date	Revision Summary
1.0	2019/07/15	Issue of first version
1.0.1	2020/7/13	1. Fix the Effective Date of v1.0 2. Add CA certificate information(1.3.1) 3. Add contact information(1.5.2) 4. Certificates issued on or after 24 August 2017 MUST NOT have a Validity Period greater than 398 days.(6.3.2.2) 5. Fix the URL of repository Website(2.1) 6. Revision of Sections 1.5.3, 4.5.1, 4.8.1, 5.3.7, 5.7.1, 6.2.5, 6.2.6, 6.2.10, 7.3.1, 9.2.1 and 9.6.4. 7. Amendments are made in Section 1.3.1, 3.2.2.2, 4.9.10, 4.9.12 and 7.1.4.2 to comply with Baseline Requirements (v1.7.0) and Mozilla Root Store Policy (v2.7).
1.0.2	2021/9/30	1. Revision of Section 1.2. According to this version, adjust the version information, announcement date and release URL. 2. Revision of Section 2.2. Add GTLSCA CPS as the way for GTLSCA to publish certificate information. 3. Revision of Section 4.2.2. Delete the rules regarding the credential application materials include the gTLDs under the scenario of GTLSCA refuse to sign and issue certificates. 4. Revision of Section 6.2.6. Modify the scenario of the CA's private key imported and exported into the HSM and add the transmission protecting way. 5. Revision of Section 6.6.1. Fix the content of system research and development control. 6. Revision of Section 6.7. Add the rules regarding network security control of GTLSCA.

		7. In response to the implementation of ACME mechanism, revise the following sections: ● Section 3.2.2.2: Add the method of Organization Authentication for ACME mechanism. ● Section 3.2.2.2: According to the B.R(section 3.2.2.4.19), add the method of domain verification for ACME mechanism. ● Section 4.2: Add the procedure of certificate application for ACME mechanism. ● Section 4.2.1: Add the procedure of certificate application for ACME mechanism. ● Section 4.3.1: Add the procedure of certificate issuance for ACME mechanism. ● Section 4.4: Add the procedure of certificate acceptance for ACME mechanism. 8. View BR version 1.7.1 to 1.7.6 and Mozilla Root Store Policy version 2.7.1, and revise the following sections: ● Section 2.3: Add the update frequency of GTLSCA CPS. ● Section 4.9.5: Add the situations that GTLSCA shall complete the revocation within one calendar day after acceptance of the certificate revocation request. ● Section 4.9.12: According to Mozilla Root Store Policy, revise other specific requirements in the event of key compromise. ● Section 6.1.1.2: Add the situation that GTLSCA shall reject a certificate application. ● Section 6.1.5: The size, in bits, of RSA keys must be evenly divisible by 8. ● Section 7.1.4.1: Revise the explanation for Name Encoding

		● Section 7.1.4.1: Revise the explanation for Name Encoding ● Section7.2.2: Add explanation for CRL and crlEntry Extensions. ● Section7.3: Add explanation for OCSP Profile. ● Section 9.12: add amendments of GTLSCA CPS version number after regular annual review. ● Revise appendix 3. 9. Revise misprint, pleonasm, conjunction, translate term and missing content and also adjust text layout. All modifications do not affect the original intention. Revise section include: Summary, Chapter 1, section 1.4.3, 2.1, 2.2, 3.2.2.2, 3.2.5, 4.1.2, 4.2, 4.2.1, 4.3.1, 4.4, 4.7, 4.9.5, 6.1.6, 6.1.7, 6.2.2, 6.6.1, 6.6.2, 7.1.2.1, 7.1.2.2, 7.1.4.2, 7.3 and 7.3.2.
1.0.3	2023/3/9	1. In line with the transfer of GPKI certificate-related businesses from the National Development Council to the Ministry of Digital Affairs, the administrative organization "National Development Council" is changed to “Ministry of Digital Affairs", and the abbreviation "NDC" is changed to "MODA” as well. 2. Amendment is made in Section 1.2 on the version information, publication date and download URL according to this revision. 3. Update contact information in Section 1.5.2. 4. Amendments are made in the following Sections to reflect the revisions of the BR versions 1.7.7 to 1.8.4: ● Section 3.1.5: organizationalUnitName (abbreviated as OU) is prohibited in the subscriber certificate. ● Section 5.4.1: The unit responsible for keeping relevant records should cover its delegated third

		parties, and the type of events to be recorded should be added. ● Section 5.4.3: The retention period of audit log is modified to at least 2 years. ● Section 5.5.1: The unit responsible for archiving relevant records should cover its delegated third parties. ● Section 7.1.4.2: comply with the BR that the FQDN must be composed of P-Labels and NR-LDH Label, and the OU field is prohibited. ● Revise Appendix 3 and update the BR version information that GTLSCA CPS complianced.
1.0.4	2024/3/6	1. Revised Section 1.2: Adjusted the version information, announcement date, and publication URL according to this revision. 2. Revised Section 4.4: Modified the default setting for certificate acceptance. In case of any objections, the applicant must submit a request for revocation. 3. Revised Section 6.1.1.1: Provided clarification on the qualified auditors presented by BR, which should include members of the management committee or certified auditing firms. 4. Revised Section 7.1.2: Amended the term "this infrastructure" to "ePKI." 5. Revised Appendices 1 and E: Amended the term "this infrastructure" to "ePKI." 6. Reviewed BR versions 1.8.5 to 2.0.2 and made the following revisions: ● Appendix 1-C: Definition of cross certificates. ● Appendix 1-E: Definition of end entities and ePKI RootCA. 7. Revised Appendix 3: Updated the BR version information reviewed by GTLSCA CPS.

1.0.5	2025/03/05	Amendments are made on Sections 1, 1.1, 1.2, 1.4.1, 1.5.1, 2.1, 2.2, 3.2.2.2, 4.2.1, 4.9.1, 4.10.2, 7.1.2.1, 7.1.2.2, 7.1.4.2, 7.2.2, 7.3, 7.3.2, 7.3.3 and Appendix 1.
1.0.6	2025/09/23	1. Revised Section 1.2 to reflect this update, including adjustments to version information, announcement date, and publication URL. 2. Revised Sections 1.2, 1.3.1, 1.4.1, 1.4.2, 2.1, 2.2, 3.2.2.2, 3.2.8, 4.2.1, 4.5.1, 4.9.1, 5.7.1 and 6.5.1. 3. Revised Appendix 3 to include the updated BR versions from this review cycle, covering versions 2.1.4 to 2.1.7.

Contents

1 Introduction

The Government TLS Certification Authority Certification 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 (Baseline Requirements) issued by the CA/Browser Forum (https://www.cabforum.org).

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 GTLSCA.

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

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

GTLSCA follows the official version of the Baseline Requirements. As for the effective date of each item of information in the official version, GTLSCA shall be complying (see Appendix 3). If GTLSCA CPS conflicts with forum regulations such as TLS certificate issuance and management, the provisions announced by the CA/Browser Forum shall prevail.

The Ministry of Digital Affairs (MODA) 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. This CPS is not authorized to be used by CAs outside 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: 1.0.6
3. Publication date: September 23, 2025
4. Download URL: https://gtlsca.nat.gov.tw/download/GTLSCA_CPS_v1.0.6_eng.pdf.
5. Certificate Policy Object Identifier (CP OID):
   - CP OID (Assurance level 3)：「1.3.6.1.4.1.23459.100.0.3」
   - CA/Browser Baseline Requirements CP OID ：「2.23.140.1.2.2」

1.3 Key Participants

The key participants of GTLSCA are:

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

1.3.1 GTLSCA

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

1. Government TLS Certification Authority - G1
   - Certificate SN:
     00 99 6d 5f e9 ad e1 6c dc 8e cd bf ed b1 4a 32 95
   - Thumbprint(SHA1):
     b2d151a768d30c3b99d86b8b25815608c28ab2cb
   - Thumbprint(SHA256):
     9d1cda1b9ef395afce7de0fe74de6d9ff5e0d2a43789116c00c
     6ba5bf44b9823
   - Not Before: 2019-07-19 14:46:45 (UTC+8:00)
   - Not After: 2031-08-19 04:46:45 (UTC+8:00)
   - Public Key Algorithm/ Key Length: RSA 4096 with sha256

GTLSCA has ceased issuing TLS certificates as of March 10, 2025.

1.3.2 Registration Authority

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 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 refer to the entities in the certificate subject name on issued certificates. For GTLSCA, subscribers are the government agencies (organizations) and units on the 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 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 Related Parties

The Data Communications Branch of Chunghwa Telecom Co., Ltd. has been commissioned by the MODA to undertake the establishment, maintenance and operation of the GTLSCA system.

1.4 Applicability

1.4.1 Appropriate Certificate Uses

TLS certificates issued by GTLSCA are primarily used in the Transport Layer Security (TLS) protocol as a security mechanism for identity authentication, allowing relying party to identify the domain name and managing entity of the subscriber’s internet server.

1.4.2 Prohibited Certificate Uses

1. man-in-the-middle TLS traffic interception;
2. applications or businesses that may result in bodily harm, psychological distress, or cause significant harm to social order and public interest; and
3. explicitly prohibited or excluded by other relevant laws or the competent authorities for specific applications/business purposes.

Subscribers are expected to comply with all requirements of all applicable browser root policies, including revocation periods of 24 hours and 5 days as specified herein.

1.5 Contact Details

1.5.1 Organization Administering the Document

Chunghwa Telecom Co., Ltd. (CHT).

1.5.2 Contact Information

- E-mail: egov@service.gov.tw
- Email for certificate problem report: gca@gca.nat.gov.tw
- Phone: 0800-770-707
- Address: No. 143, Yanping S. Rd., Zhongzheng Dist., Taipei City 100057, Taiwan (R.O.C.)

1.5.3 CPS Statement Examination and Approval

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

1.5.4 CPS Modification Procedure

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

1.6 Definitions of Terms and Abbreviations

See Appendix 1 Glossary and Appendix 2 English Acronyms.

2 Publication and Repository Responsibilities

2.1 Repository

The GTLSCA repository is responsible for the publication and storage of certificates and certificate revocation lists (CRLs) issued by GTLSCA, and this CPS. GTLSCA offers a certificate repository and query service for subscribers and relying parties, accessible via:

https://gcp.nat.gov.tw/views/AnnDownload/download.html.

The repository will resume normal operation within two working days if unable to operate normally for some reason.

2.2 Publication of Certification Information

GTLSCA shall take responsibility for making the following information publicly accessible in its repository:

1. This CPS;
2. Certificates issued by GTLSCA;
3. CRLs;
4. Privacy protection policy; and
5. The latest external audit report (as specified in Section 8.6); and
6. Provide test webpages (valid, expired, and revoked) that allow users to confirm the format and verify that GTLSCA has the capability for periodic automatic renewal.

2.3 Publication Frequency and Time

1. This CPS is reviewed and updated annually and may be published at the repository in days after being reviewed and approved by the eCA.
2. GTLSCA must issue and publish at least one CRL per day.

2.4 Access Controls

1. GTLSCA has established an information security protection mechanism that prevents 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 GTLSCA server database.

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

3 Identification and Authentication Procedures

3.1 Names

3.1.1 Types of Names

1. The subject name of certificates conforms to the distinguished name (DN) of 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 and the Fully Qualified Domain Name shall be recorded in full.
3. 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 Anonymous or Pseudonymous Names of Subscribers

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)
- commonName(abbreviated as CN)
- serialNumber

3.1.6 Trademark Identification, Authentication and Role

Not applicable.

3.1.7 Name Claim Dispute Resolution

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 Registration

3.2.1 Proof of Private Key Ownership

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 Organization Identity Authentication Procedure

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. 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. Automatic certificate reissuance mechanism

   GTLSCA uses the Automatic Certificate Management Environment (ACME) protocol complying with RFC 8555 to provide the application of automatic certificate reissuance for subscribers. Subscribers must submit the application with their valid government agency (organization) and unit certificate IC card for the first time and complete the identify authentication and the registration of identification key of the host through the dedicated ACME registration service. In the subsequent execution of automatic certificate reissuance, this identification key will be used as the basis for identity authentication.

3.2.2.2 Domain Name Ownership Authentication

1. When the subscriber applies for a certificate, GTLSCA follows the section 3.2.2.4 of the official version of the Validation of Domain Authorization or Control in Baseline Requirements 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 TLS certificates. If its dedicated fully qualified server name has a risky name, the 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:

This method of validation confirms to Section 3.2.2.4.12「Validating Applicant as a Domain Contact」 of the Baseline Requirements.

A. The competent authority of 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 MODA verifies the domain was registered by the applicant and the subscriber possesses the control rights and GTLSCA conducts identity authentication in accordance with section 3.2.2 Organization Identity Authentication Procedure.

C. Once the FQDN has been validated using this method, GTLSCA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

D. Effective January 15, 2025: - When issuing Subscriber Certificates, GTLSCA MUST NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period. - When obtaining Domain Contact information for a requested Domain Name GTLSCA: - if using the WHOIS protocol (RFC 3912), MUST query IANA's WHOIS server and follow referrals to the appropriate WHOIS server. - if using the Registry Data Access Protocol (RFC 7482), MUST utilize IANA's bootstrap file to identify and query the correct RDAP server for the domain. - MUST NOT rely on cached 1) WHOIS server information that is more than 48 hours old, or 2) RDAP bootstrap data from IANA that is more than 48 hours old, to ensure that it relies upon up-to-date and accurate information.

(2) Verification by domain contact email

This method of validation confirms to Section 3.2.2.4.2「Email, Fax, SMS, or Postal Mail to Domain Contact」 of the Baseline Requirements.

A. GTLSCA sends out an email containing a random value to the domain 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. 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. Once the FQDN has been validated using this method, GTLSCA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

E. Effective January 15, 2025: - When issuing Subscriber Certificates, GTLSCA MUST NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period. - When obtaining Domain Contact information for a requested Domain Name GTLSCA: - if using the WHOIS protocol (RFC 3912), MUST query IANA’s WHOIS server and follow referrals to the appropriate WHOIS server. - if using the Registry Data Access Protocol (RFC 7482), MUST utilize IANA’s bootstrap file to identify and query the correct RDAP server for the domain. - MUST NOT rely on cached 1) WHOIS server information that is more than 48 hours old, or 2) RDAP bootstrap data from IANA that is more than 48 hours old, to ensure that it relies upon up-to-date and accurate information.

F. Effective July 15, 2025: - GTLSCA MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method

MUST NOT be used to issue Subscriber Certificates.

(3) Change through specific web content

This method of validation confirms to Section 3.2.2.4.18 「Agreed-Upon Change to Website v2」 of the Baseline Requirements.

A. GTLSCA provides the specific web changes containing random values and the applicant must specific lists ("/.well-known/pki-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.

C. The random value must not appear in the request used to retrieve the file

D. GTLSCA must receive a successful HTTP response from the request (2xx HTTP status code must be received).

E. GTLSCA does not support the HTTP redirect.

F. This method is NOT suitable for validating Wildcard Domain Names.

G. Meanwhile, GTLSCA implements Multi-Perspective Issuance Corroboration (MPIC) as specified in Section 3.2.8 to perform validations. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

(4) Validation of the domain authentication or control for automatic certificate reissuance mechanism

This method of validation confirms to Section 3.2.2.4.19「Agreed-Upon Change to Website – ACME」of the Baseline Requirements.

A. GTLSCA confirms the applicant’s control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555.

B. The random value used for the validation in this mechanism must not be used for more than 30 days from its creation.

C. GTLSCA must receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

D. GTLSCA does not support the HTTP redirect.

E. This method is NOT suitable for validating Wildcard Domain Names.

F. Meanwhile, GTLSCA implements MPIC as specified in Section 3.2.8 to perform validations. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

3.2.3 Individual Identity Authentication Procedure

Not applicable.

3.2.4 Unverified Subscriber Information

Unverified subscriber information may not be written on the certification.

3.2.5 Verification of Rights and Responsibilities

1. When applying for a certificate, the subscriber shall follow the regulations as defined in Section 3.2.2.1 and submit the application by the official document, the valid government agency (organization) and unit certificate IC card, or automatic certificate reissuance mechanism.

2. 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 Account Delivery Criteria

No stipulated.

3.2.7 Information Accuracy

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 information.

3.2.8 Multi-Perspective Issuance Corroboration

From March 15, 2025, GTLSCA will perform MPIC for the required domain authorization or control validation and CAA record checks in accordance with Section 3.2.2.9 of the Baseline Requirements. MPIC can assist to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before certificate issuance.

Quorum Requirements Table

# of Distinct Remote Network Perspectives Used	**# of Allowed non-Corroborations**
2-5	1
6+	2

Phased Implementation Timeline:

- **Effective March 15, 2025**, GTLSCA must implement MPIC using at least 2 remote Network Perspectives. GTLSCA may proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective (“non-corroborations”) is greater than allowed in the Quorum Requirements table above.
- **Effective September 15, 2025**, GTLSCA must implement MPIC using at least 2 remote Network Perspectives. GTLSCA MUST ensure that the requirements defined in Quorum Requirements Table above are satisfied. If the requirements are not satisfied, then GTLSCA MUST NOT proceed with issuance of the Certificate.
- **Effective March 15, 2026**, GTLSCA must implement MPIC using at least 3 remote Network Perspectives. GTLSCA MUST ensure that the requirements defined in Quorum Requirements Table above are satisfied, and the remote Network Perspectives that corroborate the

Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then the CA MUST NOT proceed with issuance of the Certificate.

- **Effective June 15, 2026**, GTLSCA must implement MPIC using at least 4 remote Network Perspectives. GTLSCA MUST ensure that the requirements defined in Quorum Requirements Table above are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then the CA MUST NOT proceed with issuance of the Certificate.
- **Effective December 15, 2026**, GTLSCA must implement MPIC using at least 5 remote Network Perspectives. GTLSCA MUST ensure that the requirements defined in Quorum Requirements Table above are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then the CA MUST NOT proceed with issuance of the Certificate.

3.3 Rekey Request Identification and Authentication

3.3.1 Routine Rekey Identification and Authentication

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

3.3.2 Rekey Identification and Authentication after Certificate Revocation

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

3.4 Certificate Revocation Application Identification and Authentication

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

4 Certificate Lifecycle Operation Specifications

4.1 Certificate Application

4.1.1 Certificate Applicants

Personnel authorized by government agencies (organizations).

4.1.2 Registration Procedure and Obligations

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 this 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. Immediately 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 chapter 3 Certificate Lifespan Operation Specifications. The subscriber shall bear the relevant legal liability for use of the certificate prior to its revocation.

4.2 Certificate Application Procedure

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

5. If the applicant applied for certificate by ACME, the certificate application procedure will be completed through ACME.

4.2.1 Implementation of Identification and Authentication Functions

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

(3) If the applicant applied for certificate by ACME, the applicant’s certificate IC card issued by GCA will be use for identification and authentication. The identification key pair of applicant’s web server will be registed to be the basis of authentication.

2. Domain ownership authentication

(1) 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) Most GTLSCA subscribers use the government service network to register government domains (.gov). However, some are subscribers to other types of domains. TLS certificate application review and control all must comply with the requirements in the official version of the Baseline Requirements so GTLSCA has no high-risk certificate application problem.

Prior to issuing a TLS certificate, GTLSCA made the following checks for each dNSName in the subjectAltName extension of the certificate to be issued.

1. Certification Authority Authorization (CAA)

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

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

(2) No DNS resource record of the CAA.

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

2. MPIC attempts

   Please refer to Section 3.2.8 for details. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

4.2.2 Certificate Application Approval or Rejection

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

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 GTLSCA.

4.2.3 Certificate Application Processing Time

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, GTLSCA completes certificate issuance work within one working day.

4.3 Certificate Issuance Procedure

4.3.1 GTLSCA Work at the Time of Certificate Issuance

1. General Procedure

   After 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, GTLSCA issues the certificate and notifies the subscriber by email.

2. ACME

   After GTLSCA and its RA receive the certificate application from ACME, the review procedures in Chapter 3 Identification and

Authentication Procedure regulations are followed. The certificate application review and issuance procedures are as follows:

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

(2) The certificate will be delivered to the user from ACME. After the user comfirm the certificate, it is regarded as accepting the certificate.

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

4.3.2 GTLSCA Notification of Certificate Applicant

1. The certificate applicant is notified by email after certificate issuance.
2. The certificate applicant may check the certificate application progress at the CA website.
3. If approval is not given for certification issuance, the certificate applicant shall be notified by email or telephone and the reasons for the rejection shall be clearly explained.

4.4 Certificate Acceptance Procedure

1. 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, GTLSCA considers the certificate applicant to have accepted the certificate, then GTLSCA issues the certificate and announces it at the repository.
3. If the certificate applicant finds incorrect content on the certification, GTLSCA or RA shall be notified and submitted a certificate revocation request immediately.
4. If the applicant applied for certificate by ACME, the applicant should comfirm the Subject Name and Subject Alternative Name aftern certificate issuing. The certificate revocation should be applied within 30 calendar days, otherwise it will be regarded as accepting the certificate.

4.4.1 Certificate Acceptance Criteria

After the certificate applicant checks the certificate subject name and alternate name is free of errors and accepts the certificate, GTLSCA uses this as a basis for certificate acceptance.

4.4.2 GTLSCA Certificate Publication

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 GTLSCA Certificate Issuance Notification to Other Entities

Certificates issued by GTLSCA are published at the repository.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Use

1. Subscriber key pairs shall be generated in complies with Section 6.1.1 and the subscriber must have control 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 Public Key and Certificate Use by Relying Parties

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.
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 Extension

GTLSCA does not offer certificate extension.

4.6.1 Circumstances under which a Certificate is Extended

Not applicable.

4.6.2 Certificate Extension Applicant

Not applicable.

4.6.3 Certificate Extension Procedure

Not applicable.

4.6.4 Notification of Subscriber Extension Issuance

Not applicable.

4.6.5 Certificate Extension Acceptance Criteria

Not applicable.

4.6.6 CA Certificate Extension Publication

Not applicable.

4.6.7 GTLSCA Certificate Extension Issuance Notification to Other Entities

Not applicable.

4.7 Certificate Rekey

Refers to regenerating a key pair and using the original registration information to apply to GTLSCA for certificate issuance.

4.7.1 Circumstances under which a CA Rekey is Conducted

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 Certificate Rekey Applicants

1. GTLSCA certificate rekey

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

2. Subscriber certificate rekey

   Personnel authorized by the government agency (organization).

4.7.3 Certificate Rekey Procedure

1. 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 Subscriber Certificate Rekey Issuance Notification

Follow regulations in section 4.3.2 GTLSCA Notification to Certificate Applicants.

4.7.5 Certificate Rekey Acceptance Procedure

1. 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 GTLSCA Certificate Rekey Publication

GTLSCA publishes the completed rekeyed certificate at the repository or transmits it by email to the subscriber.

4.7.7 GTLSCA Notification to Other Entities after Rekey

GTLSCA publishes the certificate to the repository after rekey.

4.8 Certificate Modification

4.8.1 Circumstances under which is Certificate is Modified

GTLSCA does not allow subscribers to modify certificates.

4.8.2 Certificate Modification Applicants

Not applicable

4.8.3 Certificate Modification Procedure

Not applicable

4.8.4 Issuance Notification for Subscriber Certificate Modifications

Not applicable

4.8.5 Certificate Modification Acceptance Criteria

Not applicable

4.8.6 GTLSCA Certificate Modification Publication

Not applicable

4.8.7 GTLSCA Certificate Issuance Notification to Other Entities

Not applicable

4.9 Certificate Suspension and Revocation

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

4.9.1 Circumstances under which a Certificate is Revoked

4.9.1.1 Circumstances for Revoking a Subscriber Certificate

GTLSCA shall revoke a certificate within 24 hours if one or more of the following occurs:

(1) The subscriber requests in writing to the CA that they wish to revoke the certificate;

(2) The subscriber notifies GTLSCA that the original certificate request was not authorized and does not retroactively grant authorization;

(3) GTLSCA obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise;

(4) GTLSCA is made aware of a demonstrated or proven method that can easily compute the subscriber's private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or

(5) GTLSCA obtains evidence that the validation of domain

authorization or control for any FQDN or IP address in the certificate should not be relied upon.

GTLSCA should revoke a certificate within 24 hours and must revoke a certificate within 5 days if one or more of the following occurs:

(1) The certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

(2) GTLSCA obtains evidence that the certificate was misused;

(3) GTLSCA is made aware that a subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

(4) GTLSCA is made aware of any circumstance indicating that use of a FQDN or IP address in the certificate is no longer legally permitted (e.g., a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

(5) GTLSCA is made aware of a material change in the information contained in the certificate;

(6) GTLSCA is made aware that the certificate was not issued in accordance with these requirements or this CP/CPS;

(7) GTLSCA determines or is made aware that any of the information appearing in the certificate is inaccurate;

(8) GTLSCA's right to issue certificates under these requirements expires or is revoked or terminated, unless GTLSCA has made arrangements to continue maintaining the CRL/OCSP Repository;

(9) Revocation is required by this CP/CPS; or

(10) GTLSCA is made aware of a demonstrated or proven method

that exposes the subscriber's private key to compromise or if there is clear evidence that the specific method used to generate the private key was flawed.

GTLSCA may at its own discretion revoke subscriber certificates under the aforementioned circumstances.

4.9.2 Certificate Revocation Applicants

Certificate revocation applicants:

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

Subscribers, relying parties, application software vendors and other third-party organizations may submit a certificate problem report to GTLSCA. If one believes a certificate should be revoked, explain the reason for revocation in the report. 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 Certificate Revocation Procedure

4.9.3.1 Certificate Revocation Method

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 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, 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 CRL and the certificate status information is published at the repository before the next publication of the CRL at the latest and until the revoked certificate expires.
2. 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. GTLSCA accepts certificate problem reports and provides certificate problem replies 24/7.

3. 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. 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 Grace Period for Certificate Revocation Requests

Referring 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. GTLSCA may extend the certificate revocation grace period depending on the circumstances.

4.9.5 GTLSCA Certificate Revocation Request Processing Time

In principle, 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 GTLSCA.
2. The subscriber notifies GTLSCA and reports that the original certificate request was unauthorized, and reauthorization will not be given.
3. GTLSCA verifies subscriber private key spoofing, counterfeiting or compromise.
4. GTLSCA is made aware of a demonstrated or proven method that can easily compute the subscriber’s private key based on the public key in the certificate.
5. GTLSCA verifies the domain authorization or control verification method for the fully qualified domain name is untrustworthy.

4.9.6 Certificate Revocation Request Checking by Relying Parties

Before the certificate is issued by GTLSCA, relying parties shall first check the CRL or OCSP reply message published by 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. GTLSCA must reissue the CRL after certification revocation work is completed.

4.9.8 Maximum Delay Time for CRL Publication

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

4.9.9 Online Certificate Revocation / Status Check Service

1. GTLSCA provides certificate inquiry and download, CRL and OCSP inquiry services.
2. GTLSCA provides OCSP response messages conforming to RFC 6960 and RFC 5019 specifications from the Online Certificate Status Protocol Responder (OCSP Responder).
3. GTLSCA uses its private signing 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 Online Certificate Revocation Check Requirement

1. Relying parties must verify the certificate validity using the CRL or OCSP inquiry service.
2. GTLSCA provides the OCSP service, and the OCSP responder operated by GTLSCA supports the HTTP-based POST and GET methods, as described in RFC 6960 and RFC 5019.

3. GTLSCA updates the OCSP responses prior to one-half of the validity period, and the validity period of the OCSP responses is greater than or equal to 8 hours and less than 16 hours.

4. A certificate serial number within an OCSP request may be one of three options, which are "assigned", "reserved" and "unused". The “assigned” certificate serial number means the serial number of the certificate issued by GTLSCA; the “reserved” certificate serial number is the serial number of precertificates required for issuing TLS/SSL certificates; and the certificate serial number that does not meet the aforementioned conditions is the "unused" certificate serial number.

5. If the OCSP responder receives a request for the status of a certificate serial number that is “assigned”, the responder shall respond with the status at that time of the certificate assigned with that serial number.

6. If the OCSP responders receive a request for the status of a certificate serial number that is “unused”, the responder shall not respond with a "good" status. GTLSCA shall monitor the responder for such requests as part of its security response procedures.

4.9.11 Other Forms of Revocation Announcements

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

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

4.9.12 Other Specific Requirements in the Event of Key Compromise

1. The method used as proof of the compromise of the subscriber's private key is as follows:

   (1) The subscriber is responsible for investigating whether his/her private key has been compromised. After having confirmed, the subscriber shall inform GTLSCA of the event. GTLSCA will revoke the certificate concerned according to the procedures set forth in Sections 4.9.3 of this CPS.

   (2) When a third party submits the proof of key compromise, GTLSCA shall conduct the event according to the procedures set forth in Sections 4.9.3.3 of this CPS. The acceptable methods of proof of this event are the following:

      A. Confirming the third party’s possession of the private key by signing a challenge provided by GTLSCA using the compromised private key.

      B. Submitting the private key via a secure and trusted channel.

2. If a subscriber certificate is revoked due to key being compromised, the certificate will be listed on the CRL with reason code keyCompromise (1).

4.9.13 Circumstances under which a Certificate is Suspended

Use of TLS certificates may not be suspended in accordance with the Baseline Requirements.

4.9.14 Certificate Suspension Applicants

Not applicable

4.9.15 Certificate Suspension Procedure

Not applicable

4.9.16 Certificate Suspension Period Restrictions

Not applicable

4.10 Certificate Status Service

4.10.1 Service 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. GTLSCA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.
2. GTLSCA maintains an online 24x7 repository that application software can use to automatically check the current status of all unexpired certificates issued by GTLSCA.
3. GTLSCA maintains a continuous 24x7 ability to respond internally to a high-priority certificate problem report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a certificate that is the subject of such a complaint.

4.10.3 Optional Functions

No stipulated.

4.11 Service Termination

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 Private Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practice

1. GTLSCA’s private signing 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 Practice

GTLSCA does not support session key encapsulation and recovery.

5 Infrastructure, Security Management and Operation Procedure Controls

5.1 Physical Controls

5.1.1 Site location and construction

The GTLSCA facility is located in Chunghwa Telecom Information Technology Group. The facilities possess physical security mechanisms including access control, security, intrusion detection and video surveillance.

5.1.2 Physical Access

1. 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 Flood Prevention and Protection

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 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 Disposal of Obsolete Equipment

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

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.

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 for each 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

Task	**Administrator**	**Officer**	**Auditor**	**Operator**	**Physical Security Controller**
Checking, maintenance and archiving of audit logs			1		1
Daily operation and maintenance of system equipment				1	1
System backup				1	1
Storage media updating				1	1
Software and hardware updates outside the certificate management system				1	1
Maintenance of the website	1				1
Maintenance operation for system virus code and vulnerability patching (Audit Host)	1		1	1	1
Maintenance of system virus and vulnerability patching (non-audit host systems)	1			1	1
Patching the anti-virus and vulnerabilities (audit system)	1		1	1	1
Patching the anti-virus and vulnerabilities (systems other than the audit system)	1			1	1

5.2.3 Identification and Authentication for each Role

1. User account numbers, passwords and IC cards are used by GTLSCA to identify and authenticate administrator, officer, auditor and operator roles.
2. A central access system is used to identify and authenticate the role of physical security controllers.

5.2.4 Assignment of Role Duties

Role assignments 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 Background, Qualifications, Experience and Security 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 Procedure

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 Education and 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 Requirements and Frequency

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

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 Contract Personnel Regulations

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

5.3.8 Supplied Documentation

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 Log 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 Event Records

The following types of events should be recorded by GTLSCA and its delegated third parties:

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. Issuance and revocation of subscriber certificates
6. Private key export other than single use keys
7. Application and verification procedures about certificate registration, revocation and status change
8. Security-related configuration setting changes
9. Account number addition, deletion and access authorization modifications
10. Certificate profile change
11. CRL profile change
12. GTLSCA server setting change
13. Physical access and site security
14. Anomalies
15. Security module life cycle management

16. Generation of CRLs
17. Issuance of OCSP Responder
18. All verification behaviors set forth in this CPS and the Baseline Requirements
19. Approval and rejection of certificate application requests

5.4.2 Log Processing Frequency

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

5.4.3 Audit Log Retention Period

GTLSCA and its delegated third parties should retain audit log for at least 2 years. At the end of the retention period, audit personnel remove the information. Substitute personnel may not perform this task.

5.4.4 Audit Log Protection

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 Procedure

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 Log Collection System

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

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

5.4.7 Notification of Event-Causing Entity

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

5.4.8 Vulnerability Assessment

GTLSCA conducts vulnerability assessments of the operating system, physical facilities, certification management system and network.

5.5 Record Archival

5.5.1 Types of Archived Records

The following types of records should be archived by GTLSCA and its delegated third parties:

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. GTLSCA 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 Archived Records

1. The retention period for archived data and the application programs used to process archived data is at least 2 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 Archived Record Protection

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 Archived Record Backup Procedure

Archived records shall be backed up at the off-site backup center.

5.5.5 Archived Record Timestamping Requirements

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 Archived Record Collection System

GTLSCA does not have an archived record collection system.

5.5.7 Procedures to Obtain and Verify Archived Records

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. 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 Key Compromise and Post-Disaster Recovery Procedures

5.7.1 Emergency and System Compromise Handling Procedure

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. To prevent delays in revoking TLS certificates, GTLSCA conducts annual large-scale certificate revocation drills. GTLSCA develops, maintains, and conducts annual tests for a Mass Revocation Plan.

5.7.2 Computer Resources, Software and Data Corruption Recovery Procedure

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 GTLSCA Signature Key Compromise Recovery Procedure

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

5.7.4 GTLSCA Security Facility Post-Disaster Recovery Work

GTLSCA holds annual drills directed at security facility post-disaster recovery work.

5.7.5 GTLSCA Revoked Signature Key Certificate Recovery Procedure

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

5.8 GTLSCA Service Termination

1. Except for those who cannot be notified, 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. 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

Subscribers must generate the key pairs on their own. GTLSCA shall reject a certificate request if one or more of the following conditions are met:

1. The key pair does not meet the requirements set forth in Section 6.1.5 and Section 6.1.6.
2. There is clear evidence that the specific method used to generate the private key was flawed
3. GTLSCA is aware of a demonstrated or proven method that exposes the applicant’s private key to compromise.
4. GTLSCA has previously been made aware that the applicant’s private key has suffered a key compromise.
5. GTLSCA is aware of a demonstrated or proven method to easily compute the applicant’s private key based on the public key.

6.1.2 Secure Delivery of the Private Key to the Subscriber

Not applicable

6.1.3 Secure Delivery of the Public Key to the GTLSC

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 GTLSCA by transport layer security protocol or another data encryption method having an equivalent security strength.

6.1.4 Secure Delivery of the GTLSCA Public Key to Relying Parties

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

6.1.5 Key Size

1. GTLSCA uses RSA keys at least 4096 bits in size and SHA-256, SHA-384 or SHA-512 hash function to issue certificates.

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

3. The size, in bits, of the RSA keys used by GTLSCA and its subscribers must be evenly divisible by 8.

6.1.6 Public Key Parameter Generation and Quality Checking

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

2. 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 generate the prime number needed for the RSA algorithm in the cryptographic module and ensure that the prime number is a strong prime.

4. According to Section 5.3.3 of NIST SP 800-89, GTLSCA confirms that the value of the public exponent used by the RSA algorithm is an odd number greater than 3 and is in the range between 216+1 and 2256-1. Additionally, the modulus also has the following characteristics: an odd number, not the power of a prime, and has no factors smaller than 752.

6.1.7 Key Usage Purposes

1. GTLSCA’s private signing keys may be only used for issuing certificate, CRL and OCSP response messages.

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

3. 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 Security Control Measures

6.2.1 Cryptographic Module Standards and Controls

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

6.2.2 Multi-Person Control of Key Splitting

1. GTLSCA uses the private key (m-out-of-n) multi-person control to be the method of private key activation/deactivation and private key splitting backup/recovery.

2. After key generation, 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. GTLSCA’s private signing keys cannot be escrowed.

2. GTLSCA does not provide subscriber private key escrow.

6.2.4 Private Key Backup

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 Archiving

1. GTLSCA's private signing keys 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. GTLSCA does not archive its private signing keys.

6.2.6 Private Key Transfer into and from a Cryptographic Module

1. GTLSCA transfers the private key into or from the cryptographic module under the following circumstances:

   (1) Recovery of key splitting backup.

   (2) Cryptographic module replacement.

2. GTLSCA private keys are encrypted or controlled complying with the multi-person control when transferred into or from the cryptographic modules.

6.2.7 Private Key Storage in the Cryptographic Module

1. Private keys are stored in a 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 Methods for Activating Private Keys

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:

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

   (4) 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 Methods for Deactivating Private Keys

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

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

6.2.10 Methods for Destroying Private Keys

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

   (1) When the old private key is no longer being used, 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 Key Pair Management Regulations

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

6.3.1 Public Key Archiving

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

6.3.2 Usage Periods for Public and Private Keys

6.3.2.1 Usage Periods for GTLSCA Public and Private Keys

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 expires.

6.3.2.2 Usage Periods for Subscriber Public and Private Key

According to the official version of Baseline Requirements, the validity of the subscriber public key certificate must not exceed 398 days.

6.4 Protection of Activation Data

6.4.1 Generation of Activation Data

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 Protection of Activation Data

1. 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 Activation Data Regulations

No stipulated.

6.5 Computer Hardware and Software Security Control Measures

6.5.1 Specific Technical Requirements for Computer Security

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 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

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 for CA security control principles.

6.6 Lifecycle Technical Controls

6.6.1 System R&D 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. The software used by GTLSCA must be checked for malicious code before using it for the first time or updating the version and performed a security scan periodically.

5. The products or programs delivered to GTLSCA should provide handover lists, test reports, and reports of source code analysis. The version controls for the programs should be also conducted.

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. Any changes to the system must be recorded and controlled.

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

6.6.3 Lifecycle Security Controls

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

6.7 Network Security Controls

1. GTLSCA implements network security control in compliance with the requirements of Network and Certificate System Security Requirements issued by the CA/Browser Forum.
2. The information in the GTLSCA internal repository is protected by digital signature and automatically transferred from the internal repository to the external repository
3. The external repository is located in the information security protection equipment’s external service area and is connected to the Internet.
4. The GTLSCA repository protects against denial of service and intrusion attacks by system patch updates and information security systems.

6.8 Timestamping

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

7 Certificate, CRL and OCSP Format Profile

7.1 Certificate Format Profile

The certificates issued by GTLSCA follow the current versions of ITU-T X.509, the Baseline Requirements, RFC 5280 or relevant regulations in their latest version.

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 Numbers

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, the Baseline Requirements, RFC 5280, ePKI and related technical specifications.

7.1.2.1 GTLSCA Certificates

GTLSCA certificate extension content is as follows:

Extension Name	Necessity	Criticality	Content
Authority Key Identifier	Required	FALSE	The SHA-1 hash value of the root CA's public key.
Subject Key Identifier	Required	FALSE	The SHA-1 hash value of GTLSCA public key.
Certificate Policies	Required	FALSE	This extension shows GTLSCA has received eCA approval and are allowed to use the certificate policy object identifier number including:

Extension Name	Necessity	Criticality	Content
			■ CP defined certificate object identifier number. ■ CA/Browser Forum defined organization verification type SSL certificate policy object identifier number 「2.23.140.1.2.2」.
CRL Distribution Points	Required	FALSE	The HTTP URL of the root CA's CRL service.
Authority Information Access	Required	FALSE	Two items of information included in this extension: ■ The HTTP URL of the root CA's certificate. ■ The HTTP URL of the root CA's OCSP responder.
Basic Constraints	Required	TRUE	Subject Type=CA Path Length Constraint=0 (GTLSCA do not issues subordinate CA certificates downwards so the pathLenConstraint extension is set to 0)
Key Usage	Required	TRUE	The content in this extension can be one of the following: ■ keyCertSign and cRLSign. (Default) ■ digitalSignature, keyCertSign, and cRLSign. (If the subordinate CA uses the private signing key to issue OCSP responses, the bits of digitalSignature, keyCertSign, and cRLSign are asserted)
Name Constraints	Prohibited	TRUE	GTLSCA does not use this extension
Extended Key Usage	Required	FALSE	Server verification (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 Certificates

The subscriber certificate extension content is as follows:

Extension Name	**Necessity**	**Criticality**	**Content**
Authority Key Identifier	Required	FALSE	GTLSCA public key SHA-1 hash value
Subject Key Identifier	Optional	FALSE	Subscriber public key SHA-1 hash value
Certificate Policies	Required	FALSE	This extension shows the certificate policy object identifier number used by GTLSCA which includes: ■ CP object identifier number. ■ CA/Browser Forum defined organization verification type SSL certificate policy object identifier number「2.23.140.1.2.2」.
CRL Distribution Points	Required	FALSE	The HTTP URL of GTLSCA's CRL service
Authority Information Access	Required	FALSE	Two items of information included in this extension: ■ The HTTP URL of GTLSCA's OCSP responder. ■ The HTTP URL of the subordinate CA's certificate.
Basic Constraints	Optional	TRUE	Subject Type= End Entity Path Length Constraint=None (GTLSCA does not use this extension)
Key Usage	Required	TRUE	digitalSignature and keyEncipherment
Extended Key Usage	Required	FALSE	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	Required	FALSE	Records the fully qualified domain names included on this TLS certificate
Signed Certificate Timestamp List	Required	FALSE	Several certificate transparency log servers reply signed certificate timestamp (SCT) are recorded in this extension

GTLSCA 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 GTLSCA.

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

1. 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 Identifier

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

7.1.4 Name Forms

The subject and issuer fields of the certificate must use the X.500 distinguished name and the name attribute type shall comply with the current version of the ITU-T X.509, the Baseline Requirements or related regulations in the latest versions. See section 3.1.5 for an explanation of certificate subject name fields.

7.1.4.1 Name Encoding

According to Section 7.1.4.1 of the Baseline Requirements, the encoded content of the issuer distinguished name field of subscriber certificates issued by GTLSCA shall be byte-for-byte identical with the encoded form of the subject distinguished name field of the GTLSCA’s CA certificate.

7.1.4.2 Subscriber Certificate Subject Information

1. The common name field in the subject’s distinguished name and each entry listed in the subject alternative name extension of subscriber certificates must contain the Fully-Qualified Domain Name validated by using the methods noted in Section 3.2.2.2.
2. If the subscriber certificate is a multi-domain 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 certificate subject alternative name extension of the subscriber certificate should have at least one FQDN, and the

format of the FQDN must meet the following requirements.

- The preferred name syntax as specified in RFC 5280 should be followed, and should not contain the underscore symbol 「_」.
- The name is composed of P-Labels and NR-LDH Labels, in accordance with Section 7.1.2.7.12 of the Baseline Requirements.

5. See the description in Section 7.1.2.2 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 Distinguished Name (DN) attributes	**Required / Optional**
subject:commonName (OID 2.5.4.3)	Optional
subject:organizationUnitName(OID2.5.4.11)	Prohibited
subject:givenName (OID 2.5.4.42)	Prohibited
subject:surname (OID 2.5.4.4)	Prohibited
subject:organizationName (OID 2.5.4.10)	Required
subject:streetAddress (OID 2.5.4.9)	Optional
subject:postalCode(OID 2.5.4.17)	Optional
subject:localityName (OID 2.5.4.7) or subject:stateOrProvinceName (OID 2.5.4.8)	At Lease one item must included
subject:countryName(OID 2.5.4.6)	Required

7.1.4.3 GTLSCA Subject Information

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

1. commonName: Name that identifies 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 GTLSCA.
3. countryName: The country where the operation site of GTLSCA

is located. It is listed as “TW” in the ISO 3166-1 international standards.

7.1.5 Name Constraints

Certificates issued by 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 Use of Policy Constraints

Certificates issued by GTLSCA do not contain policyConstraints.

7.1. 8 Policy Qualifiers Syntax and Semantics

Certificates issued by GTLSCA do not contain policyQualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

For subscriber certificates issued by GTLSCA, their critical certificate policy extension semantics must follow the regulations in the ITU-T X.509, the Baseline Requirements and RFC 5280.

7.2 CRL Profile

7.2.1 Version Numbers

GTLSCA issues CRL that comply with RFC 5280 and ITU-T X.509 v2.

7.2.2 CRL and crlEntry Extensions

1. The CRL and CRL entry extensions in the CRL issued by

GTLSCA comply with the ITU-T X.509, RFC 5280, and the Baseline Requirements.

2. The CRL and CRL entry extensions and the criticality of these extensions are described below.

(1) CRL Extensions

Extension	**Necessity**	**Criticality**	**Description**
Authority Key Identifier	Required	FALSE	The SHA-1 hash value of GTLSCA public key.
CRL Number	Required	FALSE	The sequence number of the CRL
Issuing Distribution Point	Optional	TRUE	This extension is only applicable to a partitioned CRL. It is used to identify the CRL distribution point, indicate whether the CRL covers revocation for end entity certificates only, CA certificates only, attribute certificates only, or a limited set of reason codes, and state whether or not it is an indirect CRL. The scope of the CRL only includes certificates issued by GTLSCA, and thus the indirectCRL boolean must be set to FALSE.

(2) CRL Entry Extensions

Extension	**Necessity**	**Criticality**	**Content**
Reason Code	Required	FALSE	If the CRL entry extension is used to identify the revocation reason of subscriber certificates, the reasonCode value is as follows. ➢ keyCompromise(1) ➢ affiliationChanged(3) ➢ superseded(4) ➢ cessationOfOperation(5) ➢ privilegeWithdrawn(9)

7.3 OCSP Profile

1. GTLSCA provides OCSP services in compliance with RFC 6960 and RFC 5019, and the URL of the GTLSCA OCSP service is contained in the authority information access extension of the subscriber certificates.

2. An OCSP request accepted by GTLSCA shall contain the following information:

   - Protocol version
   - Target certificate identifier

3. An OCSP response, issued by the OCSP responder, at a minimum consists of a responseStatus field indicating the processing status of the prior request. If the value of responseStatus is ‘successful’, the OCSP response must further include the other fields as follows:

Field	Description
Version	v.1 (0x0)
OCSP Responder ID	The subject distinguished name of OCSP responder
Produced Time	OCSP response sign time
Target Certificate Identifier	The contents of this field include the hash algorithm, the hash of the issuer’s distinguished name, the hash of the issuer’s public key, and the serial number of the target certificate.
Certificate Status	The meaning of certificate status value is described below: ■ 0: The status of the certificate is valid. ■ 1: The certificate has been revoked. When this status value is used, this field shall also contain the revocation time and reason of that certificate. The

	revocationReason field within the RevokedInfo of the CertStatus shall be identical to the CRLReason of the revoked certificate noted in the CRL. 2: The status of the certificate is unknown.
ThisUpdate / NextUpdate	Recommended validity period for this OCSP response, including ThisUpdate and NextUpdate
Signature Algorithm	OCSP response signature algorithm, which can be sha256WithRSAEncryption
Signature	OCSP responder signature
Certificates	OCSP responder certificate

7.3.1 Version Numbers

Version numbers comply with RFC 5019 and RFC 6960 standards.

7.3.2 OCSP Extension

1. OCSP extensions comply with RFC 5019, RFC 6960, and the Baseline Requirements.
2. Extensions in the OCSP responses shall include authority key identifier of the OCSP responder.
3. If an OCSP request contains a nonce field, the OCSP response must also contain the same nonce field.
4. The singleExtensions in OCSP responses must not include the CRL entry extension field "reasonCode" (with the OID 2.5.29.21).

7.3.3 OCSP Service Operation Specifications

GTLSCA OCSP inquiry service operation is comprised of the following:

1. At least to use the HTTP GET method to process and accept the OCSP inquiry packet transmitted by OCSP subscribers.
2. The short-term certificate used by the OCSP responder are issued and updated by GTLSCA.

8 Audits and Other Evaluation Methods

8.1 Audit Frequency or Evaluation Methods

1. GTLSCA conducts one internal audit each year.
2. GTLSCA receives one external audit each year and audit period may not exceed 12 months.
3. The standards used for the audits are WebTrust for CA and WebTrust for CA – SSL BR.

8.2 Identity and Qualifications of Auditors

1. Auditors must be authorized by WebTrust for CA signature management unit as auditors qualified to conduct audits compliant with WebTrust for CA and WebTrust for CA – SSL BR standards.
2. Auditors must be qualified information system auditors or have the same level qualifications.
3. The GTLCSA shall verify the identities of the audit personnel during the audit.

8.3 Auditor and Auditee Relations

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

8.4 Auditing Scope

1. Whether GTLSCA CPS complies with CP regulations.
2. Whether GTLSCA and RA comply with GTLSCA CPS operations.

3. GTLSCA must follow the latest version of the Baseline Requirements and randomly sample at least 3% (randomly sample one if less than one) each quarter for verification.

8.5 Response to Audit Results

1. GTLSCA makes improvements to the non-compliances and notify the original auditor after completion to conduct a re-audit.
2. 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 Scope of Audit Result Publication

1. Except for those circumstances which could result in system security risks and the stipulations in section 9.3 Confidentiality of Business Information, 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, a 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 for CA and WebTrust for CA – SSL BR 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 and Extension Fees

No fees are being collected at this time.

9.1.2 Certificate Inquiry Fees

No fees are being collected at this time.

9.1.3 Certificate Revocation or Status Inquiry Fees

No fees are being collected at this time.

9.1.4 Other Service Fees

No fees are being collected at this time.

9.1.5 Refund Request 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 Liabilities to End Entities

Not applicable

9.3 Confidentiality of Business Information

9.3.1 Scope of Sensitive 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 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 GTLSCA.
7. Other non-disclosable information as stipulated by law.

9.3.2 Scope of Non-Sensitive 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 for Protection of Non-Sensitive Information

GTLSCA follows the regulations in the Electronic Digital Signature Act, Trust Service Principles and Criteria for Certification Authorities, Trust Services Principles and Criteria for Certification Authorities – SSL

Baseline with Network Security, the Baseline Requirements 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. 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, Trust Service Principles and Criteria for Certification Authorities, Trust Services Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, the Baseline Requirements 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, 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 GTLSCA and its intellectual property are the property of 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. 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 damage 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 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 Party 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 GTLSCA.
4. In the event that normal services cannot be provided by 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 MODA, 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 GTLSCA. 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 GTLSCA.
2. GTLSCA shall issue and manage TLS certificates in accordance with the regulations in the formal version of the Baseline Requirements.
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, 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 GTLSCA failure to comply with this CPS or relevant laws and regulations, GTLSCA 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 this 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

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

9.10.2 Termination

Termination of this CPS must be resolved by the MODA and approved by GTLSCA.

9.10.3 Effect of Termination and Survival

1. Information on GTLSCA CPS validity and termination shall be announced at the GTLSCA repository.
2. After GTLSCA CPS termination, it shall remain valid until the last issued certificate expires.

9.11 Individual Notification and Communication with Participants

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

GTLSCA performs a regular annual review of the provisions of the official version of the Baseline Requirements, and an assessment is made to determine if this CPS needs to be amended. GTLSCA shall indicate that the review or the change to this CPS has been completed by incrementing the version number and adding a dated changelog entry. In the event that the TLS issuance and management regulations in this CPS conflict with the forum regulations, the regulations issued by the CA/Browser shall prevail and this CPS shall be modified accordingly. The amended version shall be implemented following approval by GTLSCA.

9.12.1 Procedure for Amendment

Amendments to this CPS are reviewed by the MODA and announced following approval by GTLSCA.

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 MODA review 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 at leaset 15 calendar days before submission to GTLSCA for examination.
2. Less significant impact: Published at the repository at leaset 7 days before submission to GTLSCA for examination.

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

9.12.2.3 Comment Reply Period

The reply period for subscribers 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 GTLSCA.
2. GTLSCA 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 GTLSCA.

9.12.3 Circumstances under which the OID Must Be Changed

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

9.13 Dispute Resolution Procedure

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

9.14 Governing Law

For disputes involving GTLSCA issued certificates, the applicable ROC laws shall govern

9.15 Compliance with Applicable Law

Related ROC laws must be followed regarding the interpretation of any agreement signed based on this CPS.

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 this CPS may not be assigned in any form to other parties without notifying 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. GTLSCA follows the regulations in the official version of the Baseline Requirements. However, if relevant regulations are in conflict with ROC law and regulations, 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 MODA review and receive GTLSCA approval. The above work must be completed within 90 days.

   (1) The related regulations in the Baseline Requirements that are in conflict with ROC laws and regulations have been

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

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

2. GTLSCA's failure to assert rights regarding the violation of GTLSCA CPS regulations does not forfeit 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 GTLSCA, GTLSCA shall bear no legal liability.

9.17 Other Provisions

No 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, 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 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 ePKI 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).

◆ **H**

- **HiPKI Root Certification Authority (HiPKI RCA):** The HiPKI Root Certificate Authority is Chunghwa Telecom's new generation Root CA, serving as the top-level CA in this hierarchical PKI. Its public key is the source of trust and will eventually replace the ePKI Root CA as the root certificate for the source of trust.

◆ **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 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 GTLSCA itself, Self-signed certificates contain 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 CRL 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

Acronym	Full Name
RA	Registration Authority
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 the Baseline Requirements referred to by the initial version of this CPS is version 2.1.3.

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 01-Jan-13	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 mentioned in Section 11.1.3	4-Aug-2014	4-Aug-2014	Compliant
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	9-May-2017	8-June-2017	Compliant

		Root and Intermediate Certificates 9			
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	9-Mar-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	16-Mar-2019	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
1.6.6	SC19	Phone Contact with DNS CAA Phone Contact v2	20-May-2019	9-Sep-2019	Compliant
1.6.7	SC23	Precertificates	14-Nov-2019	19-Dec-2019	Compliant
	SC24	Fall Cleanup v2	12-Nov-2019		
1.6.8	SC25	Define New HTTP Domain Validation Methods v2	31-Jan-2020	3-Mar-2020	Compliant
1.6.9	SC27	Version 3 Onion Certificates	19-Feb-2020	27-Mar-2020	Compliant
1.7.0	SC26	Pandoc-Friendly Markdown Formatting Changes	20-Mar-2020	4-May-2020	Compliant
1.7.1	SC30	Disclosure of Registration / Incorporating Agency	13-Jul-2020	20-Aug-2020	Compliant

	SC31	Browser Alignment	16-Jul-2020	20-Aug-2020	
1.7.2	SC33	TLS Using ALPN Method	14-Aug-2020	22-Sept-2020	Compliant
1.7.3	SC28	Logging and Log Retention	10-Sep-2020	19-Oct-2020	Compliant
	SC35	Cleanups and Clarifications	9-Sep-2020		
1.7.4	SC41	Reformat the BRs, EVGs, and NCSSRs	24-Feb-2021	5-Apr-2021	Compliant
1.7.5	SC42	398-day Re-use Period	22-Apr-2021	2-Jun-2021	Compliant
1.7.6	SC44	Clarify Acceptable Status Codes	30-Apr-2021	3-Jun-2021	Compliant
1.7.7	SC46	Sunset the CAA Exception for DNS Operator	2-Jun-2021	12-Jul-2021	Compliant
1.7.8	SC45	Wildcard Domain Validation	2-Jun-2021	13-Jul-2021	Compliant
1.7.9	SC47	Sunset subject: organizationalUnitName	30-Jun-2021	16-Aug-2021	Compliant
1.8.0	SC48	Domain Name and IP Address Encoding	22-Jul-2021	25-Aug-2021	Compliant
1.8.1	SC50	Remove the requirements of 4.1.1	22-Nov-2021	23-Dec-2021	Compliant
1.8.2	SC53	Sunset for SHA-1 OCSP Signing	26-Jan-2022	4-Mar-2022	Compliant
1.8.3	SC51	Reduce and Clarify Log and Records Archival Retention Requirements	01-Mar-2021	15-Apr-2022	Compliant
1.8.4	SC54	Onion Cleanup	24-Mar-2022	23-Apr-2022	Compliant
1.8.5	SC56	2022 Cleanup	25-Oct-2022	30-Nov-2022	Compliant
1.8.6	SC58	Require distributionPoint in sharded CRLs	7-Nov-2022	11-Dec-2022	Compliant
1.8.7	SC61	New CRL entries must have a Revocation Reason Code	1-Apr-2023	15-Jul-2023	Compliant
2.0.0	SC62	Certificate Profiles Update	22-Apr-2023	15-Sep-2023	Compliant
2.0.1	SC63	Make OCSP optional, require CRLs, and incentivize automation	17-Aug-2023	15-Mar-2024	Compliant
2.0.2	SC66	2023 Cleanup	23-Nov-2023	8-Jan-2024	Compliant
2.0.3	SC69	Clarify router and firewall logging requirements	13-Mar-2024	15-Apr-2024	Compliant
2.0.4	SC65	Convert EVGs into RFC 3647 format	15-Mar-2024	15-May-2024	Compliant
2.0.5	SC73	Compromised and weak keys	3-May-2024	1-Jul-2024	Compliant
2.0.6	SC75	Pre-sign linting	28-Jun-2024	6-Aug-2024	Compliant
2.0.7	SC67	Require Multi-Perspective Issuance Corroboration	2-Aug-2024	6-Sep-2024	Compliant
2.0.8	SC77	Update WebTrust Audit name in Section 8.4 and References	2-Sep-2024	2-Oct-2024	Compliant
2.0.9	SC78	Subject organizationName alignment for DBA / Assumed Name	2-Oct-2024	8-Nov-2024	Compliant
2.1.0	SC76	Clarify and improve OCSP	26-Sep-2024	14-Nov-2024	Compliant

		requirements			
2.1.1	SC79	Allow more than one Certificate Policy in a Cross-Certified Subordinate CA Certificate	30-Sep-2024	14-Nov-2024	Compliant
2.1.2	SC80	Strengthen WHOIS lookups and Sunset Methods 3.2.2.4.2 and 3.2.2.4.15	7-Nov-2024	16-Dec-2024	Compliant
2.1.3	SC83	Winter 2024-2025 Cleanup Ballot	23-Jan-2025	24-Feb-2025	Compliant
2.1.4	SC84	DNS Labeled with ACME Account ID Validation Method	28-Jan-2025	1-Mar-2025	Compliant
2.1.5	SC81	Introduce Schedule of Reducing Validity and Data Reuse Periods	11-Apr-2025	16-May-2025	Compliant
2.1.6	SC85	Require Validation of DNSSEC (when present) for CAA and DCV Lookups	19-Jun-2025	21-Jul-2025	Compliant
2.1.7	SC89	Mass Revocation Planning	23-Jul-2025	25-Aug-2025	Compliant

* Effective Date and Additionally Relevant Compliance Date(s)