Government Certification Authority
Certification Practice Statement
Version 1.8

Administrative Organization: National Development Council

Executive Organization: ChungHwa Telecom Co., Ltd.

2015

Contents

SUMMARY

In compliance with the Certification Practice Statement bylaws of the Taiwan Digital Signature Act, the following is a description of key aspects of the Government Certificate Authority Certification Practice Statement (GCA CPS):

1. Competent Authority Approval Number: Jing-shang no.

2. Certificate Issuance:

(1) Types: Three types of certificates (including for digital signature use and crytographic use certificate) of government organization, unit and affiliated server application software.

(2) Assurance level: The three types of assurance level certificates defined by the Certificate Policy in accordance with the Government Public Key Infrastructure (GPKI).

(3) Applicability:

Applicable to identity authentication and data encryption of electronic related application service, and assuming malicious subscribers would intercept or temper with the network information including possible information about money transaction.

Subscriber and the relying parties must exercise discretion in using the GCA issued certificates and exclude the practice statement constraints and prohibited certificate applicability.

3. Major liability matters:

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

(2) Regarding the liability of damages arising from the use of

certificates by the subscriber or the relying parties, the liability of the GCA shall be limited to that set down in relevant laws.

(3) The GCA assumes no liability for any damages arising from a force majeure or other events non-attributable to the GCA.

(4) Government Certification Authority Certification Practice Statement (hereinafter referred to as GCA CPS) is formulated in accordance with the Certificate Policy for the Government Public Key Infrastructure (hereinafter referred to as CP GPKI) and abides by relevant regulations of the Guideline for Certification Practice Statement bylaw of the Digital Signature Act. The Statement describes how the Government Certification Authority (hereinafter referred to as the GCA) complies with requirement of the Certificate Policy Assurance Level 3 in carrying out the issuance and administration of three types of public key certificates (hereinafter referred to as Certificate) by government organization, unit and its subordinate server applications.

1.1 Overview

As stipulated by the Certificate Policy, the Government Public Key Infrastructure (hereinafter referred to as GPKI) , Level 1 Subordinate CA is responsible for issuance and administration of three types of certificates (including certificates for signature and encryption/decryption use) by government organization, unit and its subordinate server applications.

The CPS delineates how GCA proceeds according to Assurance Level 3 in issuing and managing the certificates in compliance with the Certification Policy (CP). This CPS only applies to the entities related to the community of GCA, such as GCA, Registration Authority (RA),

Subscribers, Relying Parties and Repository.

The GCA's SSL type certificate issuance and management agree to compliance with the official version of the Baseline Requirements of the Issuance and Management of Publicly-Trusted Certificates published by the CA/Browser Forum: http://www.cabforum.org. In the event of contradiction between the SSL type certificate issuance and management and the forum, provisions announced by the CA/Browser Forum shall take precedence.

The National Development Council (NDC) is the administrative organization of GCA and is responsible for the formulation and revision of GCA CPS. The CPS may go into effect only after obtaining the permission of the competent authority of the Ministry of Economic Affairs (MOEA) per the Electronic Digital Signature Act. The CPS does not authorize its use by CAs outside the GCA. The CA shall be solely responsible for any problems arising from the use of the CPS by itself.

1.2 CPS identification

The practice statement is named Government Certification Authority Certification Practice Statement, version 1.8, published on_____, 2015. You may obtian the latest version of the statement from the website below: http://gca.nat.gov.tw/download/GCA_CPS_v1.8.pdf.

The CPS is formulated according to the Certificate Policy and GCA operates in compliance with requirement of the assurance level 3 of the Certificate Policy. Its object identifier name is id-tw-gpki-certpolicy-class3Assurance, and object identifier code is {id-tw-gpki-certpolicy 3}. (Refer to the Certificate Policy.)

1.3 Key members and applicability

Relevant members of the GCA comprises of:

(1) Government Certification Authority (GCA)

(2) Registration Authority (RA)

(3) Certification Authority (CA)

(4) Repository

(5) End Entity (EE)

1.3.1 Government Certification Authority (GCA)

GCA is the first level CA of infrastructure, complies with assurance level 3 of the Certificate Policy and is responsible for the issuance and management of the three types of certificates of the government organization, unit and its subordinate server applications.

1.3.2 Registration Authority (RA)

GCA will set up a Registration Authority (RA) for collecting and verifying subscriber identity and registration work of relevant information related to certification. The RA will be formed by a number of RA Counters to be set up at GCA or its licensed unit. The RA Counter will be staffed by an RA Officer (RAO） to be responsible for business related to certificate registration, suspension application, restoration application and revocation application.

An RA Server will be installed at the RA and be responsible for verifying the identity of the RA Officer and for managing the registration counter. The RA Server will be administered by the RA Administrator. The RA Administrator will set up account number and authority for the

RA Officer on the RA Server, and produce and issue the RA officer IC card （hereinafter referred to as the RAO IC card）. An RA private key will be installed in the RA Server for communication between the RA Server and the GCA Server and to be protected by the RA private key signature.

1.3.3 Certification Authority (CA)

The token used by the CA is primarily IC card and the GCA will assign the relying CA for IC card issuance. The IC card issuance operation comprises of key pair generated internally in the IC card, and randomly set up the initial personal identity number (PIN) for the IC card, and deliver the application data and public key to the GCA via a safe conduit for issuing certificate, write the certificate onto the IC card and print out the card.

The CA will be responsible for mailing the IC card to the subscriber.

1.3.4 Repository

The repository is responsible for publishing the certificates issued by the GCA, CARL and other relevant certificate information.

Aside from setting up, maintaining and operating the repository, the GCA will post the issued certificates to the Government Directory Service (GDS).

The repository provides round-the-clock service. Its website is: http://gca.nat.gov.tw/

1.3.5 End Entity

1.3.5.1 Subscriber

GCA subscribers refer to entities of the Certificate Subject Name of the certificate issued. The GCA is responsible for issuing 3 types of

certificates, namely, government organization, unit and its subordinate server, and the subscribers are the government organization and unit.

The token used by government organization and unit subscriber is primarily the IC card but other hardware cryptographic module may also be used. Each token may simultaneously store two types of certificates for digital signature and encryption and decryption use. Each government organization or unit may only apply for one primary card but may apply for a number of secondary cards as required. Each primary card or secondary card stores two key pairs, one key pairs for digital signature use and another for encryption/decryption use, thereby the GCA will have two types of certificates for digital signature use and encryption/decryption use for each primary or secondary card.

Server application certificate is not differentiated by primary and secondary cards and may apply for a number of certificates as required. Usage of the key of the certificate may be for digital signature or encryption and decryption, and for both usages if required.

The subscriber shall follow the identification and authentication procedure of section 3.1 for initial registration in applying for the government organization or unit certificate primary card, and shall reapply following the same procedure in the event of loss or expiration of the primary card.

Upon obtaining the primary card, the subscriber may follow the identification and authentication procedure in section 3.1 at initial registration and apply for a secondary card, or apply online for the secondary card via digital signature of the primary card, and may apply for a number of secondary cards as required.

1.3.5.2 Relying Parties

A relying party is the entity that relies on the validity of the binding

nature of the certificate subject name to a public key.

Prior to using the certificate issued by the GCA, the relying party is responsible for deciding how to check the validity of the certificate by checking the appropriate certificate status information. The relying party may use the certificate for following operations only upon proving the certificate is valid:

(1) To verify the integrity of a digitally signed electronic document,

(2) To identify the creator of the electronic document,

(3) To establish confidential communications with the holder of the certificate.

1.3.6 Certification Service by Outsourcing

NDC has commissioned ChungHwa Telecom Co., Ltd. (CHT) to perform the establishment, operation and maintenance work for GCA.

1.3.7 Applicability

1.3.7.1 Certificate Applicability

Certificates issued and managed by GCA including government organization, unit and its subordinate server applications may also comprise of certificates both for digital signature use and encryption/decryption use.

The GCA issued certificates conform to assurance level 3 of the Certificate Policy and apply to identity authentication and data encryption for relevant applications of the e-government. It is assumed that the delivered information possibly comprises of money transaction which may be intercepted or tempered by malicious users on the internet.

The primary card of government organization and unit may represent

the authority for various uses but the secondary card is for specific use only.

The server application certificate may be used in Secure Socket Layer (SSL) communication protocol and for developing dedicated server applications or providing time stamping service for the server applications.

1.3.7.2 Certificate Usage Limitations

In using the private key the subscriber must exercise discretion about the secure computer environment and the relying application system so as to avoid impairing its rights by malicious hardware and software theft or erroneous use of the private key.

Prior to using the certificate issued by the GCA, the relying party must assure the type of certificate, whether it is a primary or secondary card, its assurance level and whether the usage of the key conforms to application requirement.

The relying parties shall assure the critical and non-critical certificates and extensions in accordance with the X.509 specifications.

Prior to using the certification service provided by GCA, the relying parties must carefully read the Practice Statement and at the same time pay attention to revision of the Statement.

1.3.7.3 Circumstances for Prohibiting Use of Certificate

(1) Crime

(2) Control of military orders for nuclear, biological, and chemical weapons control

(3) Operation of nuclear equipment

(4) Aviation and its control system

1.4 Contact

1.4.1Certification Practice Statement and Administrative Organization

The GCA is responsible for formulating the various provisions of the CPS. The CPS formulation and revision shall be published upon approval by the competent authority of the Ministry of Economic Affairs pertinent to the Digital Signature Act.

1.4.2 Contact Information

You are recommended to contact the GCA if you have recommendations or subscribers reporting on loss of the key. For contact telephone, postal and email addresses please go to http://gca.nat.gov.tw/

1.4.3 CPS Approval

In accordance with relevant provisions of the Digital Signature Act, the CPS must obtain approval of the competent authority of the Ministry of Economic Affairs pertinent to the Digital Signature Act before providing certification service.

2 General Provisions

2.1 Obligations

2.1.1 GCA Obligations

(1) Ensuring that its own operations meet the provisions of the Assurance Level 3 of the CP and the CPS.

(2) Carrying out identification and authentication procedure for certificate application.

(3) Issuing and publishing certificates.

(4) Revoking certificates as needed.

(5) Issuing and publishing Certification Authority Revocation Lists (CARLs).

(6) Identifying and authenticating the CA and RA personnel.

(7) Securely generating the CA private keys.

(8) Ensuring safekeeping of the GCA private keys,

(9) Supporting RA in carrying out relevant certificate registration operations.

2.1.2 RA Obligations

(1) Provide certificate application service

(2) Carry out certificate application identification and authentication procedures

(3) Securely deliver application information and public key to GCA

(4) Notify subscribers and relying parties the GCA and RA obligations

(5) Notify subscribers and relying parties that it is imperative to conform to relevant requirements of the CPS in accepting or using the GCA issued certificates

(6) Carry out RA officer identification and authentication procedures

(7) Securely generate RA private keys

(8) Safekeeping the RA private keys

2.1.3 CA Obligations

(1) Securely generate subscriber key pairs in the IC card according to section 6.1.1.1 requirements

(2) Randomly set the initial PIN code of the IC card

(3) Write the certificate onto the IC card and print the card

(4) Mail the subscriber IC card

(5) Provide IC card opening operation

(6) Execute card management operation

2.1.4 Subscriber Obligations

(1) Abide by CPS regulations and assure the provided application information is correct

(2) Upon approving and issuing the certificate by the GCA, the subscriber should accept the certificate according to section 4.3 requirement

(3) Upon accepting the GCA issued certificate, the subscriber indicates confirming the certificate content is correct and, in the event of errors in certificate information, the subscriber should take initiative to notify the GCA in accordance with section 1.3.7 governing use of the certificate.

(4) Properly keep and use the private key.

(5) Follow provisions in Chapter 4 if you require to suspend, resume, revoke or renew the certificate. In the event of leaking information of the private key or losing the key, and require to revoke the certificate, it is imperative to immediately notify the GCA but the subscriber must still assume legal responsibility in using the certificate before the mishap.

(6) Prudently select a secure computer environment and a reliable application system, and the subscriber should assume responsibility if the relying party's rights are impaired due to the computer environment or the application system.

(7) The server application certificate issued by the GCA has the subject certificate as the target object, and the holder or licensed user of the target object is the subscriber. In the event of transfer of property right or usage right of the target object, the subscriber shall revoke his or original certificate and reapply for a new certificate.

(8) In the event the GCA fails to operate normally, the subscriber should seek other ways to complete his or her legal acts and should not be used as an excuse of entering a plea against the other party.

2.1.5 Relying Party Obligations

(1) Abiding by the provisions of this CPS when using certificates issued by the GCA or when seeking information published on the repository of the GCA.

(2) While using the GCA issued certificate, it is essential to check

its assurance level to ascertain protection of subscriber's right.

(3) While using the GCA issued certificate, it is essential to ascertain the type of primary and secondary card and the usage of the key.

(4) While using the GCA issued certificate, it is essential to check the CARLs and assure the validity of the certificate.

(5) While using the GCA issued certificate, it is essential to check the digital signature and assure the certificate or CARLs are correct.

(6) Exercise discretion in selecting a secure computer environment and the relying application system, and the relying party assumes responsibility if its rights and interests are impaired due to reasons of computer environment or the application system.

(7) In the event the GCA fails normal operation, the relying party should speedily seek other ways for completing legal acts with other party should not be used as an excuse of entering a plea against the other party.

(8) Accepting the GCA issued certificate is an indication of understanding and agreeing with provisions of legal responsibility pursuant to the GCA, and shall comply with section 1.3.7 requirement in using the certificate.

2.1.6 Repository Obligations

(1) Regularly publishing the issued certificates, issued CARLs, and other related information in accordance with Section 2.6 of this

CPS.

(2) Publishing update information of the CPS.

(3) Follow Section 2.6.3 requirement for repository access control.

(4) Ensuring the accessibility and availability of the repository information.

2.2 Liability

2.2.1 GCA Liability

2.2.1.1 Warranties and Limitations on Warranties

The GCA warrants and promises to operate in accordance with the provisions of Assurance Level 3 of the CP and to follow CPS regulations for the issuance and revocation of certificate, posting of CARLs and maintenance of repository operations.

2.2.1.2 Disclaimer and Limitations

The GCA assumes no liability to consequences caused in use of certificate if the subscriber or relying party fails to comply with section 1.3.7 requirements.

2.2.1.3 Other Exclusions

GCA assumes no liability for any losses arising out of or relating to a force majeure or other reason not attributable to GCA.

In the event that GCA requires suspension of all or part of its certification services due to system maintenance, conversion, or expansion, GCA will announce that event on the repository of GCA and notify subscriber. The subscriber or relying party may not use this event

as a reason to request compensation from GCA.

In the event the subscriber intends to revoke a certificate for reasons set forth in section 4.4.1, it is necessary to file application with GCA according to the revocation procedure set forth in section 4.4.3, and latter shall complete the revocation operation within one working day upon receipt of application, issue the CARL and post on the repository. Prior to publication of certificate revocation, the subscriber shall take appropriate action to minimize influence on the relying party and assume responsibility for use of the certificate.

2.2.2 RA Liability

2.2.2.1 Warranty and Limitations

The RA shall comply with procedures set forth in the CPS and is responsible for collecting and verifying the identity of subscribers and engage in registration work related to certificate information. The RA will be formed by a number of RA Counters, and unless stipulated otherwise by law, GCA assumes liability for execution of registration work by the RA.

The GCA issued certificate only assures the certificate subject identity. The subscriber shall be liable for damages impaired on the relying party if former covers up facts and provides incorrect information to the RA in spite of the RA Officcer checking subscriber identity and relevant certificate information.

2.2.2.2 Disclaimer and Limitations

The subscriber or relaying party shall use the certificate within the appropriate scope set forth in section 1.3.7.

2.2.2.3 Other Exclusions

The GCA assumes no liability for any losses arising out of or relating to a force majeure or other reason not attributable to the GCA.

2.2.3 CA Liability

CA complies with CPS procedures and is responsible for generating subscriber's key pairs and relevant card issuance operation, thereby GCA is responsible for damage caused to any third party because of CA's execution of card issuance operation

2.3 Financial liability

The NDC budgets the operating expenses of the GCA and the National Audit Office of the Control Yuan audits the budget annually. The GCA currently has no insurance against the financial responsibility for indemnification. Other aspects of financial responsibility shall be in accordance with applicable law.

2.4 Interpretation and Enforcement

2.4.1 Applicable Laws

To meet requirement of GCA in execution of certificate issuance and administrative operation, the interpretation and lawfulness of relevant signed agreements shall abide by relevant laws and decrees.

2.4.2 Notification on Severability, Survival, Merger and Publication

Should it be determined that one section of this CPS is incorrect or

invalid, the other sections of this CPS shall remain in valid until the CPS is updated. The process for updating this CPS is described in chapter 8.

2.4.3 Dispute Resolution Procedures

In the event dispute arises between the GCA and subscribers, both parties shall first carry out consultation in accordance with the principle of faith, and may be settled in accordance with the GCA dispute resolution procedure (refer to http://gca.nat.gov.tw) by asking the GCA for the interpretation of related provisions in this CPS.

2.5 Fees

With concurrence of the electronic certificate promotion group of the Administration, the GCA may share cost or collect fees from subscribers and relying parties. Refer to the GCA website for fees collection and fees publication.

2.5.1 Certificate Issuance and Extension Fees

Refer to Section 2.5 Fees.

2.5.2 Certificate Checking Fee

Refer to Section 2.5 Fees.

2.5.3 Certificate Revocation and Status Checking Fee

Refer to Section 2.5 Fees.

2.5.4 Fees for Other Services

Refer to Section 2.5 Fees.

2.5.5 Refund Request

Refer to Section 2.5 Fees and Section 2.6 Publication and Repository

2.6.1 GCA Information Publication

(1) This CPS
(2) CARL
(3) Certificate for GCA itself (up to expiration of issued certificates by certificate public key and corresponding private key)
(4) Issued certificate
(5) Privacy protection policy
(6) Last audit result
(7) Most update GCA information

2.6.2 Publication Frequency

GCA issues a CARL every one day and publishes the CARL in the repository once it is issued.

2.6.3 Access Control

The GCA host is built inside the firewall and cannot directly connect to the outside. The repository host is controlled via the firewall system and connected to the GCA host databank, and access certificate information or download certificates.

The information published in the repository of the GCA as set forth in Section 2.6.1 is primarily provided for searches by subscribers and relying parties. Therefore, the information is open to public access. Access controls have been put in place to protect the repository security

as well as maintain the accessibility and availability of its repository.

2.6.4 Repositories

The GCA operates the repository by itself. In the event that the repository services were suspended, the GCA is responsible for restoring repository services in two working days. The URL of the repository is: http://gca.nat.gov.tw.

2.7 Auditing Method

2.7.1 Auditing Frequency

GCA accepts exteranl audit and irregular internal audit once every year for infrastructure. This is to assure relevant operations conform to the security requirement and procedure of this CPS.

2.7.2 Auditor Identity and Qualifications

In compliance with the Government Procurement Act, the NDC will outsource external auditing operation for GPKI and assign auditors familiar with relevant requirements of infrastructure to provide fair and objective auditing services. The GCA shall perform ID checks of auditors during auditing.

2.7.3 Auditor's Relationship to Audited Party

In collaboration with external auditing operation of infrastructure CA, the NDC will assign auditors for auditing the GCA operation.

2.7.4 Scope of Auditing

(1) Ensure GCA complies with CPS operation.

(2) Ensure CPS complies with CP requirement.

(3) Ensure RA complies with CPS and relevant requirements in operation.

2.7.5 Countermeasures for Auditing Result

If setup, maintenance and operation found not complying with CP and CPS requirement, the auditor shall take following actions:

(1) Noncompliance with records.

(2) Notify GCA about noncompliance.

(3) GCA shall immediately rectify noncomplying items and notify original auditor for reaudit.

(4) Depending on the nature, severity and time needed for correction, the GCA will decide to temporarily suspend operation, revoke certificate issuance, or take pertinent actions.

2.7.6 Scope of Publication for Audited Result

GCA will publish the last external auditing result by the Certification Authority in the repository, excluding information prone to attack of the GCA system.

2.8 Scope of Confidendiality

2.8.1 Types of Sensitive Information

Any information generated, received and kept by the GCA are considered confidential.

(1) All private keys and password for GCA operations.

(2) Safekeeping information separately held GCA keys.

(3) Without permission of NDC or compliance with the law, (the name, email address, communication address and telephone

number of subscriber information include organization or unit and its contact person) must not be made public or provide any third party for use.

(4) Records generated or kept by GCA for auditing and tracking.

(5) Auditing record and findings in the course of auditing by auditor may not be made public in part.

(6) Sensitive documents related to operation.

Personnel currently working at GCA or worked for GCA in the past and for external auditing have to keep sensitive information confidential.

2.8.2 Types of Non-sensitive Information

(1) Issued certificate, revoked certificate and CARLs published in the GCA repository are considered non-sensitive information.

(2) Identification information or other information recorded on the certificate are considered non-sensitive information, unless stipulated otherwise.

2.8.3 Disclosure of Revoked Certificate or Suspended Information

Revoked certificate or temporarily suspended information will be published in the GCA repository.

2.8.4 Disclose to Law Enforcement Officials

In the event that juridical, control or security apparatuses need access to the types of sensitive information specified in Section 2.8.1 of this CPS for the purpose of investigation or evidence collection, the procedure is subject to applicable laws but subscriber will not be notified otherwise. However, the GCA reserves the right to collect reasonable fees from the

inquirer to cover the expense of providing such information.

2.8.5 Disclosure Upon Subscriber Request

Subscriber may use certificate and private key to inquire about its own certificate application information per item 3, Section 2.8.1; however, GCA reserves the right to collect reasonable fees from subscriber.

2.8.6 Other Circumstances of Information Disclosure

Will not provide for commercial use; other circumstances of information disclosue shall comply with applicable law.

2.8.7 Privacy Protection

The GCA shall comply with relevant laws and decrees in accordance with the personal information protection system in handling subscriber’s application information.

2.9 Intellectual Property Right

The GCA retains all intellectual property rights in and to its own key pairs and key shares. The token used by government organization, unit certificate subscribers is IC card or other media. Key pairs generated by the GCA trusted CA or self-generated, the intellectual property of the key belongs to respective government organization, unit. SSL certificate keys self-generated by the government organization, unit, the intellectual property right belongs to respective government organization, unit.

The GCA retains all intellectual property rights to the certificates and CARLs issued by the GCA.

The GCA will ensure the correctness of the names of subscribers but

will not assure the ownership of the intellectual property right of the subscriber name. In the event of dispute in the the registered trademark, the subscriber should resolve the dispute in accordance with applicable laws and notify the GCA of the result of the dispute resolution in order to protect its own rights.

The NDC and Chunghwa Telecom Co., Ltd. jointly retain all intellectual property rights in and to the relevant documents written in the execution of GCA certificate practice. The NDC and Chunghwa Telecom Co., Ltd. jointly own the intellectual property right of the CPS. This CPS can be downloaded from the GCA repository for free, and can be, to the extent permitted by the Copyright Act, reproduced or distributed for free provided that the copy is intact and indicate copyright belongs to the NDC and Chunghwa Telecom Co., Ltd.. Those who reproduce or distribute this CPS should not charge a fee for this CPS itself and should not restrict the access to this CPS. In no event will the NDC or Chunghwa Telecom Co., Ltd. be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any improper usage or distribution of this CPS.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject name of the certificate issued by CA conforms to the Distinguished Name (DN) of X.500.

3.1.2 Need for Names to be Meaningful

The government organization, unit certificate subject name must comply with the organization constitution, organization provisions, organization rules and applicable laws and decrees.

The SSL certificate distinguished name comprises of the certificate subject name (the SSL owner or licensed user), common name, SSL name and serial number, and the GCA SSL compiled identification code.

3.1.3 Rules for Interpreting Various Name Forms

According to the certificate profile in the technical specification of GPKI, rules for interpreting various name forms should comply with the Name attribute definition of ITU-T X.520.

3.1.4 Uniqueness of Names

The GCA X.500 distinguished name is:

C=TW, O=Executive Yuan, OU=Government Certification Authority

To give uniqueness to the certificate subject name issued by GCA, following name format is used:

(1) Government organization certificate

C=TW

L=County, city name (optional field, applicable to local government only)

L=Town, township name (optional field, applicable to local organization or unit)

O=Legal name of organization

OU=Legal name of affiliated organization (optional field, may have multilayers)

(2) Government unit certificate

C=TW

L= County, city name (optional field, applicable to local government only)

L=Town, township name (optional field, applicable to local organization or unit)

O= Legal name of organization

OU=Legal name of affiliated organization (optional field, may have multilayers)

OU=Legal name of affiliated unit

A. SSL Certificate

C=TW

L= County, city name (optional field, applicable to local government only)

L= Town, township name (optional field, applicable to local organization or unit)

O= Legal name of organization.

OU= Legal name of affiliated organization or unit (optional field, may have multilayers)

CN=SSL name (possibly domain name of SSL, internet address or other language name)

serialNumber=SSL ididitification code

3.1.5 Name Claim Dispute Resolution Procedure

In the event of dispute with regard to subscriber name, the organization act, organization provisions, organization constitution or other relevant laws and decrees shall apply for resolution. And in the event of dispute in right claim to domain name or network address, the subscriber should resort to legal procedures for handling and report the result of handling to the GCA.

3.1.6 Trademark Identification, Authentication and Role

Nonapplicable.

3.1.7 Proof of Private Key Ownership

(1) Government organization, unit certificate

If the subscriber uses an IC card as token, the GCA trusted CA will generate key pairs on its behalf, and at certificate issuance the CA will deliver the public key to the GCA via a secure channel, thereby the subscriber is not required to prove that it owns the private key.

However, if the subscriber uses other token and generates key pairs by itself, and uses the key pairs to generate the PKCS#10 certificate application file, apply signature, and turn over the certificate application to the RA. Then, the RA will use the subscriber public key to authenticate the signature of the certificate application file to prove ownership of the private key by the subscriber.

(3) SSL Certificate

The subscriber generates key pairs by itself, then uses the key to

generate the PKCS#10 certificate application file, apply signature, and turn over the certificate application file to the RA at application. The RA will use the public key to authenticate the signature of the certificate application file for proof of ownership of the corresponding private key by the subscriber.

3.1.8 Authentication of Organization Identity

(1) Application in general

Subscriber should file certificate application and (including the name and address of the government organization and unit, etc.) in official document. The GCA will assure the organization and unit truly exists and verify the document is true.

(2) Applying for secondary card with certificate primary card

Subscriber with primary card may apply online for a secondary card, and the RA will verify the digital signature of the primary card as a way of authenticating subscriber identity.

(3) Replacement of certificate IC card upon expiry

Upon expiry of the IC card, replacement may be applied in general as mentioned in section (1) and may also apply online. The RA will inspect the digital signature of the expired IC card in order to authenticate subscriber identity, and check the government directory service system to assure the organization and unit truly exists.

(4) Replace certificate in compliance with CP

Certificate replacement because of policy factor (such as government reorganization, administration demarcation or change

of naming rule by the higher organization of the subscriber), application may be done in official document by the higher organization of the subscriber with permission by the GCA. The RA will check the official document of the higher organization is true.

3.1.9 Personal Identity Authentication Procedure

Nonapplicable.

3.1.10 Hardware Device or Server Software Authentication Procedure

Subscriber shall file application for certificate under the identity of equipment administrator and the authentication procedure shall follow section 3.1.8 for handling.

3.1.11 Email Authentication Written in Certificate

(1) IC card certificate

Upon obtaining the certificate IC card, subscriber may propose writing its email address onto the certificate.

Upon filing application online with certificate IC card by subscriber, the GCA will check its digital signature as authentication of subscriber's identity, and send the email verification letter to the certificate email address.

Subscriber shall use the verification letter content reply system to verify it truly owns and controls the email address.

(2) Non-IC card certificate

If required, subscriber may jointly apply for non-IC card

certificate and simultaneously writing email address onto certificate.

Aside from checking certificate application information, the GCA shall also send the email verification letter on writing the email address onto the certificate.

Subscriber shall use the verification letter content reply system to verify it truly owns and controls the email address.

3.1.12 Identification Procedure for Owner of Domain Name

The GCA should follow the General Application procedure as set forth in section 3.1.8 for authenticating the organization is true when subscriber applies for SSL Certificate. Also, the GCA may use following method to check that the host domain name truly exists and belongs to and registered under the applicant

- Government WHOIS host-government Chinese/English domain name registration system (https://rs.gsn.gov.tw)
- TWNIC Whois Database (http://whois.twnic.net.tw)

3.2 Certificate Rekey and Extension

3.2.1 Certificate Rekey

Certificate rekey refers to issuing one new certificate having same features and assurance level of the old certificate.

Except for new and different public key (corresponding to the new and different private key) and different serial number, the new certificate also may be assigned a different valid period.

Upon expiration of the subscriber’s private key, it is necessary to

renew the certificate with the GCA, and the RA will carry out identification and authentication of subscriber applying for new certificate in accordance with requirement in section 3.1.

3.2.2 Certificate Extension

The GCA prohibits extension of its issued certificates.

3.3 Rekey of Revoked Certficate

If required rekey due to revocation of subscriber's private key, it is necessary to file application with the GCA for a new certificate, and the RA shall carry out identification and authentication of subscriber applying for new certificate in accordance with requirements set forth in section 3.1

3.4 Certificate Revocation

Authenticaition procedure for application of the revoked certificate is identical to that set forth in section 3.1.

3.5 Certificate Suspension and Resumption

When applicant connects to the repository for certificate suspension or resumption, the RA system will authenticate subscriber's identity by inputing its subscriber code.

4. Operation Requirements

4.1 Procedure for Applying for Certificate

(1) Application procedure for government organization, unit certificate primary card is as follows:

A. Government organization, unit assigns appropriate personnel who represents the organization, unit in applying for certificate.

B. Certificate applicant may go to the GCA website (http://gca.nat.gov.tw/), read the Subscriber Agreement and fill out the application if it agrees to the agreement, and set its subscriber code.

C. Send the certificate application in official letter to the RA for processing.

D. Upon expiration of the certificate IC card, application for a new primary card may be done online. The RA must check the government directory service system to assure the organization truly exists before issuing certificate.

(2) Application for government organization, unit secondary cards is as follows:

A. Follows the primary card application procedure as set forth in item 1 of section 4.1.

B. Applies online and uses the government organization, unit certificate primary card digital signature to

authenticate identity. The application procedure is as follows:

(A) Certificate applicant may go to the GCA website (http://gca.nat.gov.tw/), read the Subscriber Agreement and fill out the application if it agrees to the agreement, and set its subscriber code.

(B) Upon applying digital signature to certificate primary card versus secondary card of the government organization, unit, it is necessary to upload relevant information to the RA.

C. Upon expiration of the certificate IC card, you may apply online for a new secondary card. The RA must check the government directory service system to assure the organization truly exists before issuing the certificate.

(3) SSL certificate application procedure as follows:

A. The SSL owner or licensed user represents for applying certificate.

B. The certificate applicant generates key by itself and then uses the key to generate PKCS#10 certificate application file for signature.

C. The certificate applicant may go to the GCA website (http://gca.nat.gov.tw/), read the Subscriber Agreement and fill out the application if it agrees to the agreement, and set its subscriber code and upload the PKCS#10 certificate application file.

D. Send the certificate application in official letter to the RA for processing.

(4) Certificate application procedure of subscriber's higher organization is as follows:

As stipulated in item (3), section 3.1.8, application for a new certificate is as follows:

A. The certificate applicant may go to the GCA website (http://gca.nat.gov.tw/), read the Subscriber Agreement and fill out the application if it agrees to the agreement, and set its subscriber code.

B. With permission of the GCA, the subscriber's higher organization may apply in official letter.

The certificate applicant must provide correct information in applying for a certificate. To assure government organization and unit websites are trustworthy, former must truly own government domain registered in the government Chinese and English domain name registration system if it applies for SSL certificate. Andy only then may it apply with the GCA for SSL certificate.

If government organization and unit intend to write email address into certificate, it is necessary to comply with section 3.1.11 requirement.

To assure interoperability and trustworthiness of e-government's time stamping service, the Time Stamp Authority (TSA) set up by the government organization may apply with the GCA for SSL certificate of the time stamp type.

The GCA and the RA will properly keep the subscriber's certificate

application information according to CPS requirement.

4.2 Certificate Issuing Procedure

Upon receipt of the certificate application information, the GCA or the RA will carry out following examination procedure in accordance with CPS requirement and as basis for determining issuance of certificate.

4.2.1 Government Organization, Unit Certificate Primary Card and Non-IC card Certificate

The issuance examination procedure for government organization, unit certificate primary card is as follows:

(1) The RA officer of the RA checks the truthfulness of the certificate application document and the qualifications of the applicant organization and unit (the revoked or merged organization, unit are not permitted to apply.)

(2) The certificate RA officer inspects the certificate application information, and if the subscriber wishes to apply writing the email address into the certificate, it is necessary to comply with section 3.1.11 requirement. If the information is correct, the certificate RA officer's IC card will be used to add digital signature to the certificate application information and upload relevant information to the RA.

(3) To renew the certificate primary card online, the system must use the expired certificate primary card to apply signature to the certificate application information, check the government directory service information, and make sure the information

is identical to the government and unit and then upload to the RA.

(4) Since subscriber used tokens are different, following two procedures apply:

B. If subscriber used token is IC card:

Certificate application information inspected by the RA officer will be turned over to the GCA's trusted CA for issuance operation. The issuance operation comprises of generation of key pairs inside the IC card by the CA, randomly set the initial PIN value of the IC card, and forward the application information and the public key via a secure channel to the GCA, GCA issues certificate and writes the certificate into the IC card and prints out the card. The CA is responsible for mailing the IC card to the subscriber.

C. If subscriber uses other tokens:

The GCA will issue certificate after the RA officer inspected the certificate application information and email the certificate to the subscriber.

4.2.2 Government Organization, Unit Certificate Secondary Card

Issuance and examination methods of government organization, unit certificate secondary card are as follows:

(1) Refer to aforementioned issuance and examination procedure if government organization, unit certificate primary card application procedure is used.

(2) If online application is used for government organization, unit certificate primary card digital signature, the RA will follow online digital signature for verifying the primary card.

(3) Refer to item (3), section 4.2.1 on the issuance and examination procedure if the certificate secondary card is renewed online.

If above issuance and examination fails, the GCA will reject issuing certificate. The certificate applicant may connect to the repository to check the status of certificate issuance. The GCA reserves the right to reject issuing certificate to any entity, and at the same time, does not assume responsibility for damages caused to the certificate applicant in rejecting certificate issuance.

4.2.3 Government SSL Certificate

The issuance and examination procedure for government organization SSL is as follows:

(1) The RA officer inspects the truthfulness of the certificate application document, and qualifications of the applicant organization and unit.

(2) In applying for SSL type certificate, the RA officer will complete the organization identity authentication and domain name owner authentication procedure in accordance with sections 3.1.8 and 3.1.12.

The GCA will issue certificate if the certificate application information passes inspection by the RA officer and send the certificate to the subscriber by email.

4.3 Certificate Acceptance Procedure

(1) If the subscriber uses IC card as the token, completion of IC card opening operation is an indication of accepting the certificate by the subscriber. Relevant procedure is as follows:

A. Upon receipt of the IC card, the subscriber may go to the GCA website http://gca.nat.gov.tw/ and carry out card opening operation.

B. While carrying out IC card opening, the subscriber should inspect the certificate content to make sure the information is correct. Inputting the subscriber code set at applying certificate for execution of IC card opening indicates acceptance of the certificate and will get an initial PIN code for the IC card randomly set by the CA. If the subscriber finds the certificate content is incorrect, it is imperative to stop card opening operation.

(2) If the subscriber uses other tokens, the certificate acceptance procedure is as follows:

A. Upon receipt of the certificate, the applicant subscriber should go to the GCA website: http://gca.nat.gov.tw/

B. The subscriber should inspect the certificate content and if the information is correct, then input the certificate serial number and the subscriber code set at certificate application to facilitate certificate acceptance operation. If the subscriber finds the certificate content is incorrect, it is imperative to stop the certificate acceptance

operation.

(3) Upon completing the certificate acceptance operation, the issued certificate will be published to the repository.

(4) If the subscriber fails to complete certificate acceptance operation in 90 calendar days after certificate issuance, it is considered refusing to accept the certificate and latter will be automatically revoked and not published otherwise.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances under which a Certificate may be Revoked

The subscriber should file application with the RA for revoking the certificate under one of following circumstances (but not limited to):

(1) Suspect or prove the private key has been compromised.

(2) Major change to the recorded information of the certificate which could undermine its trustworthiness. For instance, subscriber organization or unit being revoked or merged, or its distinguished name requires change which comprises of changed subscriber name or change of its higher organization.

(3) Certificate is no long needed

The GCA may directly revoke the certificate without consent of the subscriber:

(1) The information listed on the certificate is verified to be incorrect.

(2) Verified cases of unauthorized, forged or comprised private keys for subscriber signature.

(3) Verified cases of unauthorized, forged or compromised GCA private keys or the system which could undermine the trustworthiness of the certificate.

(4) Subscriber's organization or unit being terminated or merged.

(5) Subsciber's certificate being issued not in compliance with the CPS procedure.

(6) Subscriber violates the CPS or relevant laws and decrees.

(7) Per notification by the judiciary, Control Yuan or security agency.

(8) Per notification by subscriber's higher organization or competent authority of government organization.

(9) Due to involuntary name change by the government organization or unit and requires to revoke its original certificate, the GCA may consider postponing direct certificate revocation. Such certificate revocation grace period will be posted in the GCA repository.

4.4.2 Applicant for certificate revocation

(1) Subsciber who intends to revoke certificate.

(2) Subscriber's higher organization or the competent authority of government organization.

4.4.3 Certificate Revocation Procedure

(1) Subscriber or higher organization of subscriber or the competent authority of government organization assigns appropriate personnel for applying certificate revocation.

(2) Certificate revocation applicant goes to the GCA website http://gca.nat.gov.tw/, read the Subscriber Agreement, and fill out the certificate revocation application if it agrees to the content of the agreement.

(3) Submit the certificate revocation application in official letter to the original certificate RA counter for processing.

(4) Upon receipt of the official document by the RA counter, the RA officer will verify the document is true.

(5) The RA officer will inspect the application information, and if the information is correct, a digital signature will be applied to the application using the RA officer's IC card.

(6) The GCA will revoke the certificate upon passing inspection of the application information by the RA officer.

(7) For direct certificate revocation operation due to reorganization or security reasons of the GCA, the RA officer will fill out the revocation application and carry out revocation accordingly.

If aforementioned revocation application fails examination, the GCA will refuse to revoke the certificate. Upon passing examination of certificate revocation application, the GCA will complete the revocation operation in one working day.

4.4.4 Grace Period for Certificate Revocation Application

Under circumstances of item 1, section 4.4.1, the subscriber should file application within 10 working days.

4.4.5 Circumstances for Certificate Suspension

Subsciber may suspend application of certificate under following circumstances:

(1) Loss or suspect theft of token of certificate key.

(2) Subscriber determines suspension of application.

The GCA may directly suspend usage of the certificate without prior consent of the subscriber:

(1) With notification of subscriber's higher organization or the competent authority of the government organization.

(2) With notification of the judiciary.

4.4.6 Applicant for Certificate Suspension

Applicant for certificate suspension maybe as follows:

(1) Subscriber who intends to stop using the certificate.

(2) Subscriber's higher organization or the competent authority of the government organization.

4.4.7 Certificate Suspension Procedure

Based on use of different types of token the suspension is as follows:

(1) If subsciber uses the IC card as token:

A. Subscriber goes to the GCA website: http://gca.nat.gov.tw/, fill out the IC card no. and the subscriber code and apply online for suspension of certificate.

B. Upon verifying the IC card number and subsciber code are correct by the RA, apply digital signature and upload to the GCA.

C. Upon inspecting the RA digital signature, the GCA will carry out certificate suspension operation. Such operation will only temporarily stop use of the IC card certificate and will not affect the validity of other subscriber IC card certificate.

(2) If subscriber uses other tokens:

A. Subscriber goes online to the GCA website: http://gca.nat.gov.tw/, fill out the certificate serial number and subscriber code and apply online for certificate suspension.

B. Upon inspecting the certificate serial number and subscriber code are correct, the RA will add digital signature and upload to the GCA.

C. Upon inspecting the RA digital signature, the GCA will carry out certificate suspension operation.

If above suspension application fails the examination, the GCA will refuse to suspend the certificate. If the subscriber forgets its subscriber code, it is essential to send letter to the original RA counter for temporarily stopping application. Upon verifying the official

document is true, the RA officer will fill out application with the GCA for certificate suspension and reset the subscriber code.

4.4.8 Processing Period and Suspension Period for Certificate Suspension

Upon passing application of certificate suspension, the GCA will complete the suspension operation in one working day.

In applying for certificate suspension the subscriber is not required to state its required suspension period. The longest suspension period set by the GCA is from the time of application to its expiry.

If the subscriber cancels certificate suspension during the suspension period, it means resuming use of the certificate, and the certificate will become valid.

4.4.9 Certificate Resumption Procedure

Follow procedures below:

(1) Online application: Applicant goes online to the repository to apply for certificate resumption and upload to the RA.

(2) Offical document application: The applicant fills out the certificate resumption application, and send it in official document to the RA for processing. The RA officer will verify the application information is correct, then the RA officer will add digital signature to the application information with the IC card and upload relevant information to the RA.

Upon verifying the application information is correct, the RA adds

digital signature and uploads to the CA, and latter will immediately resume use of the certificate. If above resumption application fails examination, the CA wil refuse resumption.

4.4.10 CARL Issuance Frequency

The CARL issuance frequency is once every day, and the updated CARL will be published in the repository.

4.4.11CARL Inspection Rule

In using the CARL published by the GCA in the repository, the relying party must first check its digital signature to make sure the CARL is correct. For details about explanation on prerequisites of the relying party checking the repository for published information, refer to section 2.6.3.

4.4.12Certificate Status Online Checking Service

The GCA provides OCSP checking service and refers to the repository for explanation.

4.4.13 Certificate Status Online Checking

If the relying party cannot check CARL as required in section 4.4.10, it is imperative to use the checking service in section 4.4.11 to make sure the certificate in use is valid.

4.4.14 Other Forms of Revocation Announcement

Unavailable.

4.4.15 Checking Requirements for Other Forms of Revocation Announcements

Nonapplicable.

4.4.16 Special Requirements in the Event of Key Compromise

Follow requirements in sections 4.4.1, 4.4.2 and 4.4.3.

4.5 Security Audit Procedures

Audit logs are available for all events relating to the security of the GCA. The security audit logs shall be automatically generated by the system, or manually recorded in a logbook, and in paper form. All security audit logs shall be properly kept and made easily available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with the retention period for archiving, Section 4.6.2.

4.5.1 Types of Events Recorded

(1) Security audit

- Any changes to major audit parameters such as audit frequency, type of event audited and new/old parameter content.
- Any attempts to delete or modify the audit logs.

(2) Identification and Authentication

- Successful and unsuccessful attempts to assume a role
- Change in the tolerance of maximum number of identity authentication attempts
- Maximum number of unsuccessful identity authentication attempts during user login

- An Administrator unlocks an account that has been locked as a result of repeated unsuccessful authentication attempts
- The Administrator changes the system's identity authentication mechanism, for instance, from password to biometrics

(1) Key generation

- When the GCA generates a key (excluding key generation for a single time or only one time in usage).

(2) Private Key Load and Storage

- Loading private keys to system components

- Access of private keys stored in the GCA for all key resumption work

(3) Changes to the trusted public keys, including additions, deletions and storage

(3) Private Key Export

The export of private keys (keys used for a single session or restricted to a single session)

(4) Certificate Registration

- Certificate registration application processes

(4) Certificate revocation

- Certificate revocation application process.

(5) Approval for certificate status change

- Approval or denial of application for certificate status

change

(5) GCA Configuration

- Security-related changes to the configuration of the GCA

(6) Account Administration

- Additions and deletions of roles and users
- The access control privileges of a user account or a role are modified

(6) Certificate profile management

- Change of certificate profile

(7) CARL profile management

- Change of CARL profile

(8) Others

- Installation of the operating system
- Installation of the GCA system
- Installation of hardware cryptographic modules
- Removal of hardware cryptographic modules
- Destruction of hardware cryptographic modules
- System activation
- Logon attempts to GCA Apps
- Receipt of hardware/software

- Attempts to set passwords
- Attempts to modify passwords
- GCA's internal data backup
- GCA's internal data restoration
- File manipulation (e.g., creation, renaming, moving)
- Posting of any information to a repository.
- Access to the GCA internal database
- All certificate compromise complaints
- Certificate loading tokens
- Token delivery
- Token zeroization
- GCA Rekey

(7) Configuration changes to the GCA server involving:

- Hardware
- Software
- Operating systems
- Patches
- Security profiles

(8) Physical Access/Site Security

- Personnel access to GCA server room
- Access to GCA servers
- Known or suspected violations of physical security regulations

(9) Abnormality

- Software errors

- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Insufficient power supply
- Uninterruptible power supply (UPS) failure
- Significant and major network service or access failures
- Violations of Certificate Policy
- Violations of Certification Practice Statement

(9) Resetting operating system clock

- Software errors
- Software check integrity failures
- Receipt of improper messages
- Misrouted messages
- Network attacks (suspected or confirmed)
- Equipment failure
- Insufficient power supply
- Uninterruptible power supply (UPS) failure
- Significant and major network service or access failures
- Violations of Certificate Policy
- Violations of Certification Practice Statement
- Resetting the operating system clock

4.5.2 Frequency of Record File Processing

GCA shall review audit logs once every other month to keep track all significant events. Reviews involve verifying that the log has not been tampered with, inspecting all log entries, and investigating any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

4.5.3 Retention Period for Security Audit Data

Audit logs shall be retained for two months as well as being retained in accordance with sections 4.5.4, 4.5.5, 4.5.6 and 4.6 in the log retention management system rules.

Audit personnel are responsible for the removal of the expired audit logs. Other personnel may not perform this work.

4.5.4 Protection of Security Audit Logs

(1) Current and archived audit logs shall be protected by digital signing and encryption technologies and shall be stored on CD-R or other non-modifiable storage media.

(2) Private keys used to sign event log shall not be used for any other purpose. Use of Private keys of audit system for any other purposes is strictly prohibited. The audit system may not reveal private keys.

(1) Manual audit logs shall be moved to a safe, secure storage location.

4.5.5 Audit Log Backup Procedures

Electronic audit logs shall be backed up once per month.

(1) GCA shall periodically back up the event logs: The audit system shall automatically archive the audit trail data on a daily, weekly and monthly basis.

(2) GCA shall store event logs in a safe location.

4.5.6 Security Audit System

An audit system is built in the GCA system. Audit processes shall be activated upon GCA system startup and end only at GCA system shutdown.

If the audit system is not operating normally and the integrity of the system or confidentiality of the information protected by the system is at risk, the GCA shall temporarily stop issuing certificates until the problem is remedied.

4.5.7 Notification to Event-Causing Subject

When an event is recorded, the audit system does not need to notify the entity that caused the recorded event.

4.5.8 Vulnerability Assessments

(1) Vulnerability assessment of the operating systems.

(2) Vulnerability assessment of the physical facilities.

(3) Vulnerability assessment of the certification authority systems.

(4) Vulnerability assessment of the network

4.6 Records Archival

4.6.1 Types of Events Archived

(1) Accreditation information by GCA competent authority

(2) Certification Practice Statement

(3) Important agreements

(4) System and equipment configuration

(5) Modifications and updates to systems or configurations

(6) Certificate requests

(7) Revocation requests

(8) Receipt of certification acceptance log

(9) Token activation log

(10) Issued or published certificates

(11) GCA re-key log

(12) All issued and/or published CARLs

(13) All audit logs

(14) Other explanatory data or applications used to verify or substantiate archive contents

(15) Documentation requested by compliance auditors

(16) Organization and individual authentication data per sections 3.1.8 and 3.1.9

4.6.2 Retention Period for Archive

The retention period for GCA archive data is 10 years. Applications used to process archive data shall also be maintained for 10 years

Written documents shall be destroyed in a safe manner at the end of the archive retention period. Electronic data files shall be backed up in

other storage media and suitable protection provided or be destroyed in a safe manner.

4.6.3 Protection of Archive

(1) Addition, modification or deletion of the archives is not permitted.

(2) GCA may move archived records to another storage medium and shall provide proper protection with level of assurance not lower than the original one.

(1) Archive media shall be stored in a safe, secure storage facility.

4.6.4 Archive Backup Procedures

The backup of the archive data shall be stored in a remote backup center. (Refer to section 5.1.8)

4.6.5 Requirements for Time-Stamping of Records

Electronic archive data (such as certificates, CARLs and audit logs) including date and time related data shall be protected by proper digital signatures so that the date and time information on the inspection logs can be verified. However the date and time information in the electronic archive data are not electronic time-stamps provided by trusted third-party. Rather, it is the date and time from the computer operating system. The paper archive documentation shall be dated, and even time-stamped if necessary. The time and date on the paper documentation may not be changed unless the change is acknowledged and signed by the auditor.

4.6.6 Archive Collection System

GCA does not have an archive collection system

4.6.7 Procedures for Obtaining and Verifying Archive Information

Archive information may be obtained after formal written authorization is received.

Auditors are responsible for archive information verification. For paper documentation, date and signature authenticity is verified and digital signature is verified for electronic archive information.

4.7 Key replacement

Subscriber's private key must be replaced on a regular basis in accordance with requirement in section 6.3.2. If subscriber's certificate is not revoked, it is imperative to replace its key pairs within one month before the certificate expires, and apply to the GCA for a new certificate in accordance with requirement in section 4.1.

Before expiry of the usage period of the GCA private key for issuing certificate, it is necessary to complete key pairs for replacing the issued certificate and obtain cross-certificates issued by the GCA.

4.8 Compromise and Disaster Recovery

4.8.1 Restoration Procedure for Damaged or Corrupted Computing Resources, Software or Data

GCA shall define the recovery procedures that are used in the event that GCA computing resources, software, and/or data are corrupted. Recovery drills are held each year.

In the event that GCA computer equipment is damaged or rendered inoperative, but GCA signature keys are not destroyed, priority shall be given to restoring GCA repository operations and the reestablishment of certificate issuance and management capabilities.

4.8.2 Restoration of Revoked GCA Signature Keys

GCA shall set up recovery procedures for use in the event that the GCA signature keys are revoked. Recovery drills are held each year.

4.8.3 Restoration of Compromised GCA Signature Keys

GCA formulates the restoration procedure for compromised signature keys and carry out drills every year.

4.8.4 Recovery of GCA Security Facilities Following a Disaster

GCA carries out recovery drill of security facilities following a disaster every year.

4.9 Termination of GCA Services

In the event of termination of the GCA services, the related provisions of the Electronic Signatures Act shall apply.

In order to minimize the impact on subscribers and relying parties in the event of termination, the GCA shall:

(1) Notify all unrevoked and unexpired certificate subscribers (does not apply if notification is not possible) and publish the announcement in the repository three months before the scheduled service termination date.

(2) GCA shall revoke all unrevoked or unexpired certificates upon service termination, and retain and transfer archives in

accordance with the Electronic Signature Act.

5. Non-Technical Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The GCA facility, located at the Chunghwa Telecom Data Communication Branch, complies with facility standards for the housing of high value, sensitive information. And equipped with other physical security protection systems, including access control, security guards, video monitoring and intrusion sensors, the facility has robust protection against unauthorized access to related GCA equipment.

5.1.2 Physical Access

GCA operates physical access control at assurance level 3. There are four access control levels in the server room. On the first and second levels, there is year-round entrance and building security in place. On the third level, access is controlled to this floor using a card access control system. On the fourth level, a fingerprint recognition control system is used to control facility personnel access. The fingerprint scanner uses 3D sampling technology which is capable of detecting whether the fingerprint is from a live object by fingerprint depth and color.

The physical access control system of the GCA is able to protect the facilities from unauthorized access. There is also a monitoring system in place to control cabinet access which prevents unauthorized access to any

hardware, software, or hardware secure module in the GCA.

Portable storage devices that are brought into the facility housing are checked for computer viruses or other types of malicious software that could damage the GCA system.

Non-GCA personnel who need to enter the facility need to sign the entry log and be accompanied by GCA personnel throughout the tour.

The following checks and records need to be made when GCA personnel leave the facility to prevent unauthorized personnel from entering the facility:

(1) Make sure equipment is working normally

(2) Make sure the computer rack is locked.

(3) Check that the security access system is working

5.1.3 Electrical Power and Air Conditioning

In addition to city power, the power system at the GCA facility is equipped with a generator (with enough fuel for six days of continuous operation) and an uninterrupted power system (UPS). The system is capable of automatically switching between city power and generator and can provide at least six hours of backup power for repository data backup.

The GCA facility has constant temperature and humidity air conditioning system to provide an optimal operation environment for the operation of the GCA facility.

5.1.4 Flood Prevention and Protection

The GCA facility is located on the third or higher floor of an elevated foundation. This building has water gate and water pump protection and no history of major damage caused by flooding.

5.1.5 Fire Prevention and Protection

The GCA facility has automatic fire detection, alarm and protection system with self-activating extinguishing equipment and switches are installed at every major entrance/exit of the facility to allow manual activation by personnel on-site during emergencies.

5.1.6 Media Storage

Audit records, archives, and backups are kept in storage media for one year at the GCA facility. After one year, the data shall be moved for storage in a remote location.

5.1.7 Waste Disposal

When sensitive information and documents of the GCA as described in section 2.8.1 are no longer in use, all paper, magnetic tapes, hard disks, floppy disks, magneto-optical disks and other forms of memory shall be destroyed in accordance with the standard procedures announced by government authorities.

5.1.8 Remote Backup

Remote backup is located in Taichung, 30 km away from the GCA facility. One backup of all information including system programs and data shall be made at least once per week. Backups of modified data shall be done on the same day of the modification. The remote backup system has equivalent security controls to the GCA.

5.2 Procedural Controls

In order to protect the security of system procedures, the GCA uses procedural controls to specify the trusted roles of related system tasks, the number of persons required for each task, and how each role is identified

and authenticated.

5.2.1 Trusted Roles

In order to properly distinguish the duties of each system task and to prevent undetected malicious use of the system, the trusted role authorized to perform each system access item is clearly defined.

The five trusted roles at the GCA are administrator, officer, auditor, operator, and physical security controller. Each trusted role is administrated according to section 5.3 to prevent possible internal intrusion. Each trusted role may be performed by multiple persons but one person shall be assigned the chief role. The work performed by each role is as follows.

(1) The administrator is responsible for:

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

(2) The officer is responsible for:

- Activating or suspending certificate issuance service.
- Activating or suspending certificate revocation service.

(3) The auditor is responsible for:

- Checking, maintaining and archiving of audit records.

- Performing or supervising internal audits to ensure the GCA is operating in accordance with CPS regulations.

(4) The operator is responsible for:

- Daily operation and maintenance of system equipment.
- System backup and recovery.
- Storage media updating.
- Hardware and software updates outside of the GCA system.
- Network and website maintenance: Set up system for security, virus protection system and network security event detection and reporting.

(5) The physical access controller is responsible for:

System physical security controls (such as facility access controls, fire prevention, water protection and air conditioning systems).

5.2.2 Roles Assignments

The five trusted roles defined in section 5.2.1 must follow the rules below:

(1) A person may only assume one of the Administrator, Officer, and Auditor roles, but the person may also assume the Operator role.

(2) The physical security Controller may not concurrently assume any of the other four roles.

(3) A person serving a trusted role is not allowed to perform

self-audits.

5.2.3 Number of Persons Required Per Task

In accordance with security requirements, the number of people assigned to serve in each trusted role is as follows:

(1) Administrator: at least 3 qualified individuals

(2) Officer: at least 3 qualified individuals

(3) Auditor: at least 2 qualified individuals

(4) Operator: at least 2 qualified individuals

(5) Controller: at least 2 qualified individuals

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

Assignments	Administrator	Officer	Auditor	Operator	Controller
Installation, configuration, and maintenance of the GCA certificate management system	2				1
Establishment and maintenance of GCA certificate management system subscriber accounts	2				1
Configuring audit parameters	2				1
Generation and backup of GCA keys	2		1		1
Activating or suspending certificate issuing service		2			1
Activating or suspending certificate revoking service		2			1
Checking, maintaining, archiving audit log	2		1		1
Daily operation maintenance of system equipment	2			1	1
System backup and	2			1	1

Assignments	Administrator	Officer	Auditor	Operator	Controller
restoration operation					
Storage media update	2		1		1
Hardware/software update in addition to GCAcertificate management system		2			1
Network and website maintenance				1	1
Physical security control in configuring system					2

5.2.4 Identification and Authentication for Each Role

The GCA utilizes user account, password and group management functions and IC cards to identify and authenticate administrator, officer, auditor, operator, and controller roles as well as central access control system authorization setting function to identify and authenticate physical security controllers.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Requirements

(1) (1) Personnel selection and security assessment

- Personality assessment
- Applicant experience assessment
- Academic and professional qualifications assessment
- Verification of personnel identity
- Personnel integrity assessment

(2) Personnel evaluation management

All GCA personnel shall have their qualifications checked

before employment to verify their qualifications and work abilities. After formal employment, personnel shall receive appropriate training and sign a document accepting responsibility to perform certain duties. All personnel shall have their qualifications rechecked each year. If personnel do not pass the qualification check, a qualified individual shall be assigned to serve in this position.

(3) Appointment, dismissal and transfer

If there are changes to the employment contract, in particular employees leaving their job or at termination of employment contract, personnel are still required to uphold their duty of confidentiality.

(4) Duty of confidentiality agreement

All GCA personnel shall sign an agreement to fulfill the duty of confidentiality and sign a non-disclosure affidavit stating that sensitive information may not be disclosed orally, by photocopy, by borrow reading, by delivery, article publication or other methods.

5.3.2Background Check Procedures

The GCA shall check the related documents that verify the identity and certify the qualifications of the personnel performing the trusted roles defined in Section 5.2.1 prior to employment.

5.3.3 Training Requirements

Trusted Roles	Training Requirements

Administrator	1. GCA security clearance system. 2. Installation, configuration, and maintenance of the GCA operation procedures. 3. Set up and maintain system subscriber account operation procedure. 4. Set up audit parameters operation procedures. 5. GCA key generation and backup operation procedures. 6. Disaster recovery and sustainable business operation procedure.
Officer	1. GCA security clearance system. 2. GCA software and hardware use and operation procedures 3. Certificate issuance operation procedure. 4. Certificate revocation operation procedure. 5. Disaster recovery and sustainable business operation procedure.
Auditor	1. GCA security clearance system. 2. GCA software and hardware use and operation procedures 3. GCA key generation and backup operation procedures. 4. Audit log check, upkeep and archiving procedures. 5. Disaster recovery and sustainable business operation procedure.
Operator	1. GCA security clearance system. 2. Daily operation and maintenance procedures for system equipment. 3. Storage media updating procedure. 4. Disaster recovery and sustaible business operation procedure. 5. Network and web service maintenance procedure.
Controller	1. Physical access authorization setting procedure. 2. Disaster recovery and sustaible business operation procedure.

5.3.4 Retraining Frequency and Requirements

For GCA hardware/software upgrades, work procedure changes, equipment replacement and amendments to related laws and regulations, retraining will be arranged for related personnel and record the training status to ensure that related work procedures and regulatory changes are understood.

5.3.5 Job Rotation Frequency and Sequence

(1) A full year of service at the original position is needed before an administrator can be reassigned to the position of officer or auditor.

(2) A full year of service at the original position is needed before an officer can be reassigned to the position of administrator or an auditor.

(3) A full year of service at the original position is needed before an auditor can be reassigned to the position of administrator or officer.

(4) Only personnel with a full two years of experience as an operator as well as passing the requisite training and examination may be reassigned to the position of administrator,

officer or auditor.

5.3.6 Sanctions for Unauthorized Actions

The related GCA personnel shall accept appropriate administrative and disciplinary actions for violation of CP and CPS, or other published procedures. In the event of serious cases that resulted in damages, appropriate legal action shall be taken.

5.3.7 Employee Requirement

Aside from signing confidentiality agreement, GCA employees must have adequate knowledge and skills and moral integrity, and abide by CPS regulations in carrying out operation.

5.3.8 Provided Documents

The GCA shall make available to related personnel relevant documentation pertaining to the GPKI CP, technical specifications, the CPS, system operation manuals and the Electronic Signature Act.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

According to section 6.2.1, GCA generates key pairs using RSA algorithm within the hardware cryptographic module by means of a random number generator mechanism that complies with the requirements of FIPS140. Key output and input upon generation of the private keys from hardware cryptographic module shall comply with

requirements in sections 6.2.2 and 6.2.6.

GCA key generation shall be carried out under witness by the administration electronic certificate promotion group and relevant personnel.

6.1.1.1 Certificate Key Pairs Generation by Government Organization and Unit

Key pairs shall be generated by the GCA trusted CA if government organization and unit certificate subscribers use IC card as token. The CA shall use IC card which has passed FIPS 140 level 2 certification or equivalent security strength IC card. While generating key pairs inside the IC card, and upon completion of key pairs generation, the private keys will not be able to output from the IC card.

The government organization and unit shall generate key pairs by themselves if other tokens are used.

6.1.1.2 SSL Certificate Key Pairs Generation

In applying for SSL certificate, subscribers shall generate key pairs by themselves.

6.1.2 Private Key Secure Delivery to Subscriber

Private key shall be generated by the GCA trusted CA in accordance with requirement in section 6.1.1.1 if the government organization and unit certificate susbscribers use IC card as token. The CA will mail the IC card stored with the private key to the subscriber upon GCA certificate issuance.

6.1.3 Public Key Securely Delivered to GCA

The public key shall be delivered to the GCA via a secure channel

by the RA if the subscriber key pairs are generated by the GCA trusted CA.

However, if subscriber generates key pairs by itself, it is necessary to send the public key to the RA using the PKCS# 10 certificate application file format. The RA shall verify the subscriber truly owns the corresponding private key in accordance with requirement of section 3.1.7 and securely send the subscriber public key to the GCA.

The secure channel refers to the Secure Socket Layer, using a dedicated communication protocol or data signature and encrypted delivery such as Certificate Management Protocol certification packet with signature by the RA officer, etc.

6.1.4 GCA Public Key Delivery to Relying Parties

GCA public key shall be issued by the GRCA and posted in the GRCA repository for direct download and used by the relying parties. Before using the GCA public key certificate, the relying parties shall follow the GRCA CPS requirement and obtain the public key of the GRCA via a secure channel or self-issued certificate, then verify the GCA public key certificate signature by the GRCA to ensure the public key is trustworthy.

6.1.5 Key Sizes

The GCA uses 2048-bit RSA key and the SHA-1, SHA256, SHA384 or SHA512 hash function algorithm for issuing certificate and the subscriber uses 1024 bit or 2048 bit RSA key.

6.1.6 Public Key Paramters Generation

The public key paramter for RSA algorithm is null.

6.1.7 Key Parameter Quality Checking

The GCA adapts ANSI X9.31 algorithm or the FIPS 186-3 standard to generate the prime numbers used in the RSA algorithms. This method can guarantee that the generated prime numbers are strong prime.

Subscriber key can generate the required prime numbers using the RSA algorithm inside the IC card or other hardware/software cryptographic module but cannot guarantee the prime numbers are strong prime.

6.1.8 Key Generation by Hardware/Software

The GCA uses hardware cryptographic modules to generate random numbers, public key pairs and symmetric keys in accordance to section 6.2.1.

In using IC card that has passed FIPS 240 level 2 certification or IC card with equivalent security strength, the subscriber will generate key pairs inside the IC card or generate key pairs by using other hardware/software cryptographic modules.

6.1.9 Usage Purposes

The GCA public key certificate is issued by the GRCA wherein the certificate key usage extension is set at keyCertSign and cRLSign. And the GCA signature use private key is for issuing certificate and CARLs.

The government organization and unit certificate comprises of two key pairs for signature and decryption use.

The SSL certificate key usage may be for signature or encryption use and for both signature and encryption and decryption use if required.

6.2Private Key Protection

6.2.1Standards for Cryptographic Module

According to section 6.2.1 of CP regulations, the GCA uses hardware cryptographic modules with an FIPS140-2 assurance level 3 to generate random numbers and key pairs. The subscriber key pairs storage media may be IC card or other media.

6.2.2 Control of Key Shared by Multi-persons

GCA control of key shared by multi-persons uses the m-out-of-n LaGrange Polynomial Interpolation. It is a perfect secret sharing method, and may use sharing backup of private keys and restoration method. Such method gives the highest security to GCA private keys held by multi-persons, thereby it is also used as an activation method for private keys (refer to section 6.2.7).

6.2.3 Private Key Escrow

The GCA private key used for digital signature generation cannot be escrowed. And GCA is not responsible for keeping any subscriber's private key used for signature.

6.2.4 Private Key Backup

In accordance with section 6.2.2 private key backup is done by control of key sharing by multi-persons and uses the highly secure IC card as the storage media for secret sharing.

6.2.5 Private Key Archiving

GCA private keys used for signature cannot be archived. And GCA also does not archive any private keys of subscribers for signature use.

6.2.6 Private Key Importation into Cryptographic Module

GCA can only import the private key into the cryptographic module during key backup, restoration and replacement of the cryptographic module as required by section 6.2.2 for multi-persons control. Private key import may be encrypted or key sharing to ensure no exposure of the key throughout the course of importation. Upon completion of importation of the private key, it is imperative to destroy completely all sensitive parameters.

6.2.7 Private Key Activation

Activation of the RSA private key of GCA is by m-out-of-n control of the IC card group, and the control IC card group for different usages is kept by the administrator and the officer.

6.2.8 Private key Suspension

Suspension of the RSA private key of the GCA is by m-out-of-n IC card group.

6.2.9 Private Key Destruction

To prevent theft of the old GCA private key which affects correct issuance of certificate, GCA will not issue any certificate and CARLs using the old private key, and carry out zeroization of the memory address of the old private key stored in the hardware cryptographic module. At the same time, sharing of the old private key also will be physically destroyed.

6.3 Other Rules for Management of Subscriber Key Pairs

Subscriber shall manage its own key pairs. The GCA will not be

responsible for keeping the subscriber private key.

6.3.1 Public Key Archiving

GCA shall carry out certificate archiving according to section 4.6 for executing security control of the archiving system and will not carry out public key archiving.

6.3.2Usage Periods for the Public and Private Keys

6.3.2.1Usage Periods for GCA Public Keys and Private Keys

The GCA public and private keys are 4096 bits in size with a usage period not more than 20 years. And the usage period of private key for issuing subscriber certificate is not more than 10 years.

The usage period for public keys is limited to 30 years and private key usage period is limited to 10 years, excluding that for issuing CARLs and OCSP for checking server certificate.

6.3.2.2 Usage Periods for subscriber public and private keys

The key sizes of subscriber public and private keys are RSA 1024 bits or RSA 2048 bits. The usage period of public key certificate and private key are both not more than 5 years if the key size is RSA 1024 bits, and not more than 9 years both for public key certificate and for private key if the key size is RSA 2048 bits.

6.4 Protection of Activated Data

6.4.1 Generation of Activated Data

GCA's activated data is generated by the hardware cryptographic module and written into the m-out-of-n controlling IC card group. The activated data in the IC card is directly accessed by the card reader of the

built-in hardware cryptographic module. The IC card PIN code is being input by the built-in keyboard of the hardware cryptographic module.

6.4.2 Protection of Activated Data

The GCA activated data is being protected by the m-out-of-n controlling IC card group. The IC card PIN code is kept by the keeper and not recorded in any media. The IC card will be locked if login fails for a third time. At handover of the IC card, the new keeper will reset the new PIN code.

6.4.3 Other Rules for Activating Data.

No such rules.

6.5Computer Hardware and Software Security Controls

6.5.1Specific Technical Requirements for Computer Security

The GCA and related auxiliary systems provide the following security control functions by means of the operating system, or jointly through the operating system, software and physical protection measures as follows:

(1) Login with identity authenticated.
(2) Provide discretionary access control.
(3) Provide security audit capability.
(4) Access control restrictions for various certificate services and trusted roles.
(5) Possess identification and authentication of trusted roles and identity.
(6) Use cryptographic technology to ensure security of each communication and database.

(7) Possess secure and trusted channels for trusted roles and relevant identity identification.

(8) Possess procedure integrity and security control protection.

6.5.2 Computer Security Rating

GCA uses computer systems with security levels equivalent to C2(TCSEC), E2(ITSEC) or EAL3(CC,ISO/IEC 15408) computer operating system.

6.6 Life Cycle Technical Controls

6.6.1 System R&D Control Measures

GCA system R&D follows the quality management specifications approved by the competent authority for quality control and posted in the GCA website repository.

System development environment, testing environment and online operating environment must be clearly separated in order to prevent unauthorized access or risk of change.

All products or programs turned over to the GCA must have signed a safety warranty to make sure no backdoor or malicious programs, and provide program hardware turnover checklist, testing report and system management manual for version control of the program.

6.6.2 Security Management Controls

The GCA will not install any hardware device irrelevant to operation, network connection or component software. At installation of software for the first time, GCA will make sure the supplier provides a correct and unmodified version and automatically checks the integrity of the software on a daily basis. GCA records and controls system configurations,

modifications and function upgrade while also tests for unauthorized modifications of system software and configurations.

6.6.3Life Cycle Security Ratings

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

6.7Network Security Controls

GCA host and its internal repository are connected to exterior networks through double firewalls. The external repository is in the external service area (DMZ) outside the firewall and connected to the Internet to permit uninterrupted provision of certificates and CARL search services (except for required maintenance and backups).

The information in the GCA internal repository (including certificates and CARLs) is protected by digital signature and is transferred automatically from the internal repository to the external repository.

The GCA external repository prevents denial of services and intrusion attacks with system patch file updates, system vulnerability scanning, intrusion detection system, firewall systems and filtering routers.

6.8 Cryptographic Module Security Controls

Follow the provisions in sections 6.1 and 6.2.

7 Profile

7.1 Certificate Profile

The profile of GCA issued certificates shall comply with related GPKI technical specifications.

7.1.1 Version number

The GCA issues X.509 v3 version certificates.

7.1.2 Certificate Extension Fields

The certificate extensions field of GCA issued certificates shall comply with GPKI technical specification regulations.

7.1.3 Algorithm Object Identifiers

Any of the following algorithm OIDs may be used for signatures used on GCA issued certificates:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

(OID：1.2.840.113549.1.1.5)

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

(OID：1.2.840.113549.1.1.11)

sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}

(OID：1.2.840.113549.1.1.12)

sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}

(OID：1.2.840.113549.1.1.13)

The following OIDs must be used with the subject key algorithm for GCA issued certificates.

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

(OID：1.2.840.113549.1.1.1)

7.1.4 Name forms

The subject and issuer fields of the certificate shall comply with X.500 Distinguished Name and its attribute type shall comply with RFC5280.

7.1.5 Name Constraints

Name constraints are not used for GCA issued certificates.

7.1.6 Certificate Policy Object Identifier

The certificate policy object identifier field of the certificate shall use the OID of GPKI CP.

7.1.7 Use of Policy Constraints Extension

Policy constraints are not used for GCA issued certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by GCA shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

A ‘critical or not’ note must be made for the CP extension field contained in the GCA issued certificates in accordance with the GPKI certificate and CARL profile regulations.

7.2 CARL Profile

7.2.1Version number

GCA issues X.509 v2 CARLs.

7.2.2 CARL Entry Extensions

GCA issued CARLs shall comply with GPKI technical specification regulations.

8. CPS maintenance

8.1Change procedure

A periodic evaluation of the CPS shall be conducted each year to determine if any changes are required to maintain assurance. Revisions may be made to the CPS by document attachment or direct revision of the CPS content. If there are revisions made to the CP or changes to the OID, accompanying revisions should be made to CPS.

8.1.1Notification Not Required for Change

New typographic layout changes to the CPS may be made without notification.

8.1.2 Notification Required for Change

8.1.2.1 Change Items

Evaluation of the level of impact of the change on subscribers and relying parties:

(1) Where there is a major impact, a posting will be made in the repository for 30 calendar days before the changes are made.

(2) Where there is a minor impact, a posting will be made in the repository for 15 calendar days before the changes are made.

8.1.2.2 Notification mechanism

Changes to all items in this CPS shall be posted in the GCA repository.

8.1.2.3 Opinion Feedback Period

The opinion feedback period for changes is as follows:

(1) Where there is major impact per section to 8.1.2.1(1), the opinion feedback period will be 15 canlendar days.

(1) Where there is minor impact to section 8.1.2.1(2), the opinion feedback period will be 7 canlendar days.

8.1.2.4 Opinion Handling Mechanism

Any opinions on the proposed changes should be submitted before the deadline of the response period and should be forwarded to the GCA in the response method of the GCA repository posting. The GCA will consider relevant opinions and evaluate the changed items.

8.1.2.5 Final Posting Deadline

The CPS posted changes shall comply with sections 8.1.2.2 and 8.1.2.3 for revision, and the posting period shall be 15 calendar days as stipulated in section 8.1.2.1 until CPS revision takes effect.

8.2Publication and Notification Requirement

The revised CPS shall be posted within 7 calendar days to the GCA repository and the revision valid date shall take effect after posting unless specified otherwise.

8.3CPS Review Procedures

The CPS shall be announced by the GCA once it is approved by the competent MOEA authorities per the Electronic Signature Act. Upon publication of the revised CP, the CPS shall be revised accordingly and

submitted to the competent MOEA authorities for approval per the Electronic Signature Act.

Unless stipulated otherwise, the revised CPS shall take precedence in the event of any conflicts between the content of the revised CPS and the original CPS. If revisions to the CPS are in the form of attached document, the content of the attached documents shall take precedence in the event of any conflicts between the content of the attached document and the original CPS.