Certificate Policy for the Government Public Key Infrastructure

Version 2.0

Administrative Organization: National Development Council
Executive Organization: ChungHwa Telecom Co., Ltd.
June 14, 2019

Version Revision Log

Version	Effective Date	Description of Revised Content
2.0	2019/06/14	Update to RFC3647

CONTENTS

1. Introduction

In order to create a robust electronic government infrastructure environment, the Republic of China had established the Government Public Key Infrastructure (hereinafter referred to as "GPKI") in 2005 pursuant to ITU-T X.509 standards. The GPKI was composed of trust anchors: Government Root Certification Authority (hereinafter referred to as the "Root Certification Authority") and Subordinate Certification Authority formed by government agencies. The Certification Authority joining the GPKI shall only be a government agency whose issued certificate can be used in various network service applications.

The National Development Council (hereinafter referred to as "NDC") is the administrative agency of GPKI, which had established "Government Electronic Certification Steering Committee" to provide policy consultation. In order to provide a common specification for the management of GPKI certificates and to promote internal and external interoperability, NDC had enacted the "Certificate Policy for the Government Public Key Infrastructure" (hereinafter referred to as the "Certificate Policy").

1.1 Overview

1.1.1 Certificate Policy

The Certificate Policy was enacted pursuant to the provisions of Electronic Signatures Act and referred to international standards to serve as a basis for each Certification Authority to enact Certification Practice Statement. In order to ensure interoperability of the public key certificates, all of the Certificate Authorities joined the GPKI shall comply with the Certificate Policy.

There are 5 identity assurance level (hereinafter referred to as the "assurance level") defined under the Certificate Policy, namely: test level, AL 1, AL 2, AL 3 and AL 4, respectively. The level of assurance is higher as the number increases, where the test level is only applicable to test certificates.

The GPKI had registered Certificate Policy Object Identifier with a total of 5 assurance levels (see Section 1.2). The Certification Authority can, upon certificate issuance, choose adequate Certificate Policy Object Identifier and list it in the Certificate Policy extension fields in the certificate, so that the relying party can confirm applicability of the certificate via object identifier.

Certification Authority shall indicate the Certificate Policy Object Identifier in the extension field corresponding to the Certificate Policy of the Cross-Certificate. The relying party (please refer to Section 1.3.5 for the definition of "relying party") can confirm the corresponding relationship, in terms of Certificate Policy between the Issuing CA and the Subject Certification Authority, via the object identifier.

1.1.2 Relationship Between Certificate Policy and Certification Practice Statement

Certification Authority shall expressively state the means of compliance with the Certificate Policy's assurance level in the Certification Practice Statement.

In addition, the Certificate Policy and the SSL certificate issuing Certification Authority shall comply with the requirements of the official "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published by the CA/Browser Forum and the requirements of the items listed in that version (see Appendix 2).

1.1.3 Certificate Policy Object Identifier Used by Certification Authority

Certification Authority shall obtain NDC's consent before using the Certificate Policy's Certificate Policy Object Identifier. Any problem arising from unauthorized use shall be borne by the attributable Certification Authority.

A Certification Authority shall choose an adequate Certificate Policy Object Identifier based on the applicability of the certificate it issued and record it in the Certificate Policy's extension fields. However, the Root Certification Authority's self-signed certificate shall only serve as trust anchor's information object without the need to indicate certificate policy's object identifier. The relying party can directly trust the public key information listed in the self-signed certificate.

1.2 Document Name and Identification

(1) Name: Certificate Policy for the Government Public Key Infrastructure

(2) Version: 2.0

(3) Announcement date:

The Certificate Policy defined 5 assurance levels of Certificate Policy Object Identifier (see Schedule 1-1), which were registered in the id-tw-gpki arc. The Object Identifiers are expressively stated as follows:

id-tw OBJECT IDENTIFIER :: = {2 16 886}
id-tw-gov OBJECT IDENTIFIER :: = {id-tw 101}
id-tw-gpki OBJECT IDENTIFIER :: = {id-tw-gov 0}
id-tw-gpki –certpolicy OBJECT IDENTIFIER :: = {id-tw-gkpi 3}

Schedule 1-1 Certificate Policy Object Identifier

assurance level	name of the object identifier	object identifier value
test level	id-tw-gpki-certpolicy-testAssurance	{id-tw-gpki-certpolicy 0}
AL 1	id-tw-gpki-certpolicy-class1Assurance	{id-tw-gpki-certpolicy 1}
AL 2	id-tw-gpki-certpolicy-class2Assurance	{id-tw-gpki-certpolicy 2}
AL 3	id-tw-gpki-certpolicy-class3Assurance	{id-tw-gpki-certpolicy 3}
AL 4	id-tw-gpki-certpolicy- class4Assurance	{id-tw-gpki-certpolicy 4}

The issuance of SSL certificate (currently only available in Government Certification Authority) shall comply with the official "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published by the CA/Browser Forum. If the aforesaid official version is insistent with the Certificate Policy or Certification Authority's Certification Practice Statement, the provisions stipulated in the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" shall prevail.

The SSL certificate issued by subordinate Certification Authority shall comply with provisions stipulated in the official "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published by the CA/Browser Forum and pass the external audit of "AICPA/CPA SM/TM WebTrust Principles and Criteria for Certification Authorities–SSL Baseline with Network Security" prior to the use of organization validated SSL Certificate Policy Object Identifier defined by CA/Browser Forum in its certificate and the SSL certificate issued. The Object Identifiers are: {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)}(2.23.140.1.2.2).

1.3 Primary Members

1.3.1 Government Electronic Certification Steering Committee

The tasks of Government Electronic Certification Steering Committee are described as follows:

(1) Deliberation on the policy and Certification Practice Statement of Government Electronic Certification.

(2) Deliberation on the related technical specifications of Government Electronic Certification.

(3) Review the framework of the Government Electronic Certification system.

(4) Other administration particulars relating to the Government Electronic Certification.

1.3.2 Certification Authority

1.3.2.1 Government Root Certification Authority

The Root Certification Authority is a AL 4 GPKI Root Certification Authority. Its main duties are described as follows:

(1) The issuance and management of self-signed certificates, self-issued certificates, cross-certificates and subordinate CA certificates.

(2) The establishment of GPKI cross-certification procedures, and the issuance and management of GPKI's level one subordinate CA certificates and other Certification Authority's certificates.

(3) The publication of issued certificate and Certification Authority Revocation List in the repository and ensuring normal operation of the repository.

1.3.2.2 Subordinate Certification Authority

The tasks of the subordinate Certification Authority are described as follows:

(1) The issuance and management of Subscribers' certificates.

(2) The issuance, if necessary, of certificate to subordinate Certification Authorities based on the structural approach of the hierarchical public key infrastructure; the subordinate Certification Authorities shall not directly carry out cross-certification with non-GPKI Certification Authority.

(3) Subordinate Certification Authority shall be established, including the Authority Operator, pursuant to related provisions of the Certificate Policy.

1.3.3 Registration Authority

(1) Registration Authority is responsible for the collection and verification of subscriber identity and accuracy of related information.

(2) The Root Certification Authority shall assuming the role of a Registration Authority; subordinate Certification Authority may set up independent Registration Authority.

(3) Certification Authority shall describe the Registration Authority's operational approach in the Certification Practice Statement.

1.3.4 Subscribers

(1) Referred to the entities identified by the subject names, which have possession of the certificate's public key and its corresponding private key.

(2) In terms of certificates issued to incapacitated applications and hardware equipment, subscriber of certificate referred to the personal or organization applied for the certificate.

(3) The Certification Authority identified by cross-subject name shall be called Subject Certification Authority instead of a subscriber.

1.3.5 Relying Party

Referred to the personal or organization who/which trusting the subject name and its binding relationship with the public key and private key.

1.3.6 Other Related Members

Certification Authority may commission other organizations (such as key management center, card issuer, etc.) to assist in the processing of certificate-related operations, provided that, identity of the entrusted organization shall be expressively stated in the Certification Practice Statement, and the operation procedures, management approach, responsibility and obligations shall be formulated.

1.4 Certificate Usage

The relying party shall carefully evaluate various risks to choose the applicable certificate.

1.4.1 Applicability of the Certificate

The Certificate Policy does not mandate the applicability and applicable subject of the certificate for each level of assurance. However, in order to set norm for each Certification Authority, the advisable applicability for each level of assurance are shown in the following Schedule:

Schedule 1-2 Applicability of the Assurance Level

Assurance Level	Applicability
test level	For testing purposes only. No legal liability shall be borne for any transmitted data.
AL 1	Applicable in network environment with a low risk of malicious tampering or, when a higher assurance level cannot be provided, the identification of subscriber entity names and the assurance on the integrity of the signed documents.
AL 2	Applicable in network environment where information may be harmlessly tampered with (the chance of information being intercepted is not high).
AL 3	Applicable in network environment risker than AL 2 with interception or tampering of information by malicious users. The transmitted information includes electronic transactions.
AL 4	Applicable in network environment with high risk or the costs of recovery tampered information are high. The transmitted information includes large sum electronic transactions or highly confidential documents.

The Certificate Policy provided 3 token assurance levels for each Certification Authority and relying party. The token assurance levels are described in the follows Schedule:

Schedule 1-3 Descriptions of the Token Assurance Levels

token assurance level	descriptions
AL 1	Providing only partial assurance as to whether or not the token controller truly binded the Subscribers' accounts. Its successful single-factor or multi-factor authentication via the use of any available verification technique shall, via a secure authentication protocol, be able to confirm that the subscriber truly have possession of and control over that token. (1) Permitted token type: can use any one of the following types. ■ Memorable secret code, such as: password or personal identification number; ■ Single-factor encryption software; ■ Single-factor encryption equipment; ■ Multi-factor encryption software; ■ Multi-factor encryption equipment. (2) Requirements of the token and validator: ■ The encryption token shall use the approved encryption technology. The software token can also try to detect the possible of malicious attack to the terminal equipment (such as: installed with malicious software). If it is found, the certification in question shall be terminated. ■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack.
AL 2	Providing reliable assurance as to whether or not the token controller truly binded the Subscribers' accounts. Its authentication carried out under the secure environment of authentication protocol via the use of two authentication factors shall include the approved encryption technology. (1) Permitted token type: The verify operation shall be performed via multi-factor authentication or a combination of two types of single-factor authentication.

	■ If multi-factor authentication is taken, the available types of token include: ➢ Multi-factor encryption software; ➢ Multi-factor encryption equipment. ■ If the combination of two types of single-factor authentication is taken, it shall include a memorable secret code token and any one-time token described below: ➢ Single-factor encryption software; ➢ Single-factor encryption equipment. (2) Requirements of the token and validator: ■ Encryption token shall use the approved encryption technology. The token for government procurement shall pass FIPS 140 level 1 certification. The software token can also try to detect the possible of malicious attack to the terminal equipment (such as: installed with malicious software). If it is found, the certification in question shall be terminated. In addition, at least one type of token with replay attacks prevention capacity, such as dynamic passwords, shall be used. ■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack. ■ If equipment such as mobile device is used in the verification process, the equipment's original unlocking function (such as: fingerprint recognition or personal identification number verification) shall not be regarded as a verification factor.
AL 3	Providing highly reliable assurance as to whether or not the token controller truly binded the Subscribers' accounts. It verifies ownership of the subscriber's key via encryption protocol. The verification operation requires hardware password token and token capable of blocking from hacked validator (can also simultaneously use equipment with the aforesaid functions) and shall be carried out under the secure environment of authentication protocol via the use of two authentication factors, which shall include the approved encryption technology. (1) Permitted token type: can use a combination of any one of the following tokens.

	■ Multi-factor encryption equipment; ■ A combination of single-factor encryption equipment and memorable secret code. (2) Requirements of the token and validator: ■ The token owner and validator shall communicate with each other via authorized and securely encrypted channel to avoid man-in-the-middle attack. All encryption equipment token shall be equipped with validator capable of anti-hacking and replay attacks prevention. ■ The token shall be cryptographic module which passed FIPS 140 level 2 (or up) or is in compliance with Global Platform Trusted Execution Environment. ■ If equipment such as mobile device is used in the verification process, the equipment's original unlocking function (such as: fingerprint recognition or personal identification number verification) shall not be regarded as a verification factor.

1.4.2 Use Constraints on the Certificate

The relying party shall first decide the assurance level required for the application before choosing the right certificate for the assurance level and determine applicability of the certificate in question pursuant to provisions prescribed in Section 6.1.9 "Usage Purposes of Key".

The relying party shall check validity of the certificate by using the certificate verification methods defined by the related international standards (such as: X.509 standard or IETF RFC, etc.).

1.4.3 Prohibited Uses of the Certificate

The certificates issued by GPKI Certification Authority are not permitted to be used for the following purposes:

(1) Crime;

(2) Military command and situation, and the control of nuclear, biological and chemical weapons;

(3) Other: subject to be specified by each subordinate Certification Authority.

1.5 Contact Details

1.5.1 Establishment and Administration Body of the Certificate Policy

The establishment and administration body of this Certificate Policy is NDC.

1.5.2 Contact Information

E-mail address：gca@gca.nat.gov.tw

The phone numbers, postal address of the GRCA can be found at https://grca.nat.gov.tw/GRCAeng/index.html.

1.5.3 Certification Practice Statement Review

Certification Authority shall be in compliance with the following procedures if it intends to provide certificate issuance service to the public:

(1) The Certification Authority shall first check if the Certification Practice Statement is in compliance with the Certificate Policy related provisions before Government Electronic Certification Steering Committee's review for approval.

(2) The Certification Practice Statement shall be submitted to the competent authority of the Electronic Signatures Act for approval.

1.5.4 Procedures for the Change of Certificate Policy and Certification Practice Statement

If there is any published revision to the Certificate Policy, the Certification Practice Statement shall be revised accordingly and handled pursuant to the review procedures prescribed in Section 1.5.3.

1.6 Definitions and Abbreviations

See Appendix 1 "Term Definitions".

2 Information Publication and Repository's Responsibility

2.1 Repository

Each Certification Authority must provide at least one internet-accessible repository and ensure the availability, access control and data integrity of the repository. The repository's URL shall be specified in the Certification Practice Statement; the repository's access control shall be handled pursuant to the provisions of Section 2.4 "Access Control".

2.2 Publication of Certificate Information

Certification Authority shall publish the following contents in the repository:

(1) Certificate Policy and Certification Practice Statement;

(2) Certification Authority Revocation List or Certificate Revocation List;

(3) Providing enquiry service for the Online Certificate Status Protocol;

(4) Certification Authority's certificates;

(5) All certificates issued;

(6) Privacy policy;

(7) Other necessary and verifiable digital signature information that shall be published.

2.3 Publication Frequency or Time

(1) The frequency of publishing the Certification Authority Revocation List or Certificate Revocation List shall be subject to the provisions of Section 4.9 "Temporary Suspension and Revocation of the Certificate".

(2) Certification Authority shall, in the Certification Practice Statement, specify its statement publication frequency or time.

(3) The Root Certification Authority shall make an announcement in the repository within 7 calendar days after the approval is granted to the Certificate Policy's revised contents.

2.4 Access Control

(1) Certification Authority is entitled to determine access control method for the certificates.

(2) Certification Authority shall protection repository's information to prevent unauthorized modification.

3 Identification and Authentication

3.1 Naming

GPKI certificate's name shall include subject name and common name.

3.1.1 Type of Names

(1) The subject name shall be X.500 distinguished name (DN).

(2) Certification Authority reserves the right to approve whether to write the common name proposed in the Subscriber's certificate application into the certificate. If common name is written into the certificate, the corresponding field shall be indicated as a non-critical extension field.

3.1.2 Need for Names to be Meaningful

(1) The subject names used in the organizational and individual certificates shall be subject to the relevant laws and regulations of R.O.C. and consistent with the officially registered name.

(2) The subject name used for equipment or server application software shall be the name of the administrator of the equipment or server application software. The name shall be easy to understand and recognize.

(3) The subject name and common name used in SSL certificate shall not be an internal name or reserved IP address.

3.1.3 Anonymous or Fake-Name Subscribers

Certification Authority may, based on its needs, decide whether or not a subscriber can be allowed to use anonymous or fake name without stipulating the provision in the Certificate Policy.

3.1.4 Rules for Interpreting Various Name Forms

The name form shall be enacted in the "Government Public Key Infrastructure Certificate and Certificate Revocation List Profile" and authorized by Government Electronic Certification Steering Committee before promulgation.

3.1.5 Uniqueness of Names

For subject with same name, the Certification Authority shall, in the Certification Practice Statement, specify the use of X.500 distinguished name to ensure uniqueness.

3.1.6 Recognition, Authentication and Role of Trademarks

The subject name, include trademark's, shall be named pursuant to the related provisions of the Trademark Act of R.O.C.

3.1.7 Name Dispute Resolution Procedures

Certification Authority shall, except for those operative under test level of assurance, specify name dispute resolution procedures in the Certification Practice

Statement.

3.2 Initial Registration

3.2.1 Method of Proving the Possession of Private Key

Certification Authority shall, upon subscriber's certificate application, verify if applicant's private key pair-up with public key.

The Certificate Policy's approved methods of proving the possession of private key are as follows:

(1) When Certification Authority or Registration Authority generates key pair for the subscriber

Subscribers do not need to prove possession of private key but must undergo identification verification pursuant to Section 3.2 "Initial Registration" provisions. Certification Authority shall deliver the private key to the subscriber pursuant to Section 6.1.2 "Secure Delivery of Private Keys to Subscribers" provisions.

(2) When trusted third party generates key pair for the subscribers

Certification Authority or Registration Authority shall, pursuant to Section 6.1.3 "Secure Delivery of Public Keys to the CA" provisions, obtain the subscriber's public key from the third party via secure channel. Subscribers do not need to prove possession of the corresponding private key but must undergo identification verification pursuant to Section 3.2 "Initial Registration" provisions. Certification Authority shall deliver the private key to the subscriber pursuant to Section 6.1.2 "Secure Delivery of Private Keys to Subscribers" provisions.

(3) When the subscriber self-generates key pair

Subscriber's use of private key in signature generation shall be subject to Section 6.1.3 "Secure Delivery of Public Keys to the CA" provisions providing the generated signature to Certification Authority or Registration Authority before the Certification Authority or Registration Authority can use subscriber's public key, or NDC approved method, to verify the generated signature and prove subscriber's possession of the private key in question.

3.2.2 Authentication of Organization Identity

The authentication of organization identity shall be handled by different procedures depending on the applicable assurance level as listed in Schedule 3-1 below.

The identification and authentication procedures on Certification Authority shall be subject to the identification and authentication procedures prescribed in Schedule 3-1, which shall not be lower than the assurance level of the certificate that the Certification Authority intended to issue.

The Root Certification Authority's identification verification to subordinate Certification Authority shall be handled pursuant to AL 3 provisions.

Schedule 3-1 Authentication of Organization Identity

assurance level	authentication procedures
test level	Certification Authority may, at its own discretion, define the authentication procedures based on its needs. The Certificate Policy will not specify in this regard.
AL 1	(1) Written documentation does not need to checked. (2) Applicant only needs to provide e-mail address to apply for a certificate.
AL 2	(1) Written documentation does not need to checked. (2) Subscriber shall submit organization information, such as organization identification number, name of the organization, etc., which shall be cross-checked with CA approved information.
AL 3	(1) Authentication of government agency (organization) identity ■ Official documents shall be used for the first-time certificate application for authorization. ■ Certification Authority or Registration Authority shall, upon expiration of the agency (organization) certificate usage period, issue new certificate to that government agency (organization) upon confirmation of its existence. The method of identification verification shall be specified in the Certification Practice Statement. (2) Authentication of civil organization identity The information required to be verified for civil organization's certificate application shall include name of the organization, location and representative, and other information sufficient to identify the organization. Certification Authority or Registration Authority shall, in addition to the verification of the authenticity of the application information and representative's identity, verify that the representative has been authorized to apply for a certificate on behalf of the organization. The identity authentication can be performed by the following methods: ■ The application shall be proceeded in person at the Certification Authority or Registration Authority by representative or proxy appointed in writing. The Certification Authority or Registration Authority shall confirm authenticity of the power of attorney and verify identity of the proxy pursuant to the AL 3 provisions prescribed in Section 3.2.3 "Authentication of Individual Identity". ■ If the civil organization has completed the registration procedures pursuant to law and kept the registration, identification and authentication information, it shall submit supporting informationwhen applying for certificates without the need to go through over-the-counter process. ■ The organization representative may, if its identity has been authenticated pursuant to AL 3 provisions prescribed in Section 3.2.3 "Authentication of Individual Identity", it may submit

assurance level	authentication procedures
	certificate application online with its natural person certificate and submit supporting information for authentication.
AL 4	(1) Authentication of government agency (organization) identity Government agency (organization) shall assign a representative authorized by official documents to apply certificate in person and shall verify identity of the representative pursuant to the AL 4 provisions prescribed in Section 3.2.3 "Authentication of Individual Identity". (2) Authentication of civil organization identity The certificate shall be applied in person and attach information sufficient to identify the organization, such as name of the organization, location and representative. Certification Authority or Registration Authority shall, in addition to the verification of the authenticity of the application information and representative's identity, verify that the representative has been authorized to apply for a certificate on behalf of the organization.

3.2.3 Authentication of Individual Identity

The authentication of individual identity shall be handled by different procedures depending on the applicable assurance level as listed in Schedule 3-2 below.

Schedule 3-2 Authentication of Individual Identity

assurance level	authentication procedures
test level	Certification Authority may, at its own discretion, define the authentication procedures based on its needs. The Certificate Policy will not specify in this regard.
AL 1	Subscriber only needs to provide e-mail address to apply for a certificate.
AL 2	Subscriber shall provide personal information such as ID card number, name, etc. for authorization.
AL 3	(1) Subscriber shall provide ID card number, name and original copy of identification with photo or government issued document sufficient in proving the subscriber's identity. Application shall be processed over-the-counter in person or by a proxy appointed in writing. (2) Subscriber's application or certificate revocation shall be processed in person. (3) Certification Authority or Registration Authority shall verify the authenticity of the application information and cross-check with the information registered at the competent authority or the competent authority approved information registered by trusted third party. Subscriber who has completed the over-the-counter identification and authentication at Certification Authority, Registration Authority or CA trusted organization pursuant to the aforesaid provisions and kept supporting evidence (such as biometric data, authorized signature and/or seal, verifiable public key) of the identification and authentication, the Certification Authority or Registration Authority may allow the supporting evidence thereof to be used as the proof of identification and authentication when the subscriber apply for certificate.

assurance level	authentication procedures
AL 4	The identity authentication procedure is the same as that of AL 3, except the subscriber must apply in person.

3.2.4 Unverified Subscriber Information

The unverified subscriber information shall not listed in the certificate.

3.2.5 Confirmation of Rights and Responsibilities

Certification Authority shall, in the Certification Practice Statement, specify the ways for the applicant to be authorized to act on behalf of the subject, which shall meet the following principles:

(1) Proving that the organization truly exist through third-party identity authentication service, database, government agency, or a body of persons that has the authority and credibility.

(2) Confirming that the individual truly serves for the subject and authorized to act on behalf of the subject via face-to-face, telephone, paper-based mail, e-mail or other means.

Certification Authority shall, when the common name field is used in recording e-mail address and secure email application, specify in the Certification Practice Statement the means for the applicant to control that e-mail account.

Certification Authority shall, upon providing the application for SSL certificate, specify in the Certification Practice Statement the means to confirm the authorization of domain control authority.

3.2.6 Interoperability Standard

Certification Authority may, at its own discretion, define the interoperative standard based on its needs. The Certificate Policy will not specify in this regard.

3.2.7 Authentication of ICT Equipment or Server Application Software

(1) The information & communication technology equipment certificate or SSL certificate shall be applied by the competent authority, organization or individual pursuant to the identity authentication provisions in Section 3.2.2 or 3.2.3.

(2) Certification Authority shall, in the Certification Practice Statement, specify the means to authenticate the identity of information & communication technology equipment or server application software.

3.3 Identification and Authentication for Re-key Request

The Issuing Certification Authority shall, when the Subject Certification Authority applies for replacement of key pair, perform the identification and authentication

operations on the Subject Certification Authority pursuant to Section 3.2 “Initial Registration”.

Certification Authority shall, when subscriber of the End Entity applies for replacement of key pair, perform the identification and authentication operations on the subscriber pursuant to Section 3.3 provisions.

Schedule 3-3 Identity Authentication Provisions for Re-key

assurance level	identity authentication provisions for the re-key of subscriber certificate
test level	Certification Authority may, at its own discretion, determine identity authentication provisions for subscriber’s re-key. The Certificate Policy will not specify in this regard.
AL 1	Subscriber’s identity can be authenticated by the use of valid signing key or by the authentication operation prescribed in Section 3.2 “Initial Registration”.
AL 2	(1) Subscriber′s identity can be authenticated by the use of valid signing key or by the authentication operation prescribed in Section 3.2 “Initial Registration”. (2) If it has been more than 15 years since the initial registration, the identity authentication operation shall be repeated pursuant to the Section 3.2 “Initial Registration”.
AL 3	(1) Subscriber′s identity can be authenticated by the use of valid signing key or by the authentication operation prescribed in Section 3.2 “Initial Registration”. (2) If it has been more than 9 years since the initial registration, the identity authentication operation shall be repeated pursuant to the Section 3.2 “Initial Registration”.
AL 4	(1) Subscriber′s identity can be authenticated by the use of valid signing key or by the authentication operation prescribed in Section 3.2 “Initial Registration”. (2) If it has been more than 3 years since the initial registration, the identity authentication operation shall be repeated pursuant to the Section 3.2 “Initial Registration”.

3.3.1 Identification and Authentication for Routine Re-key

The Issuing Certification Authority shall, when Certification Authority carries out routine re-key operations, perform the identification and authentication operations on the Certification Authority pursuant to Section 3.2 “Initial Registration”.

Certification Authority shall, when subscriber of the End Entity carries out routine re-key operations, perform the identification and authentication operations on the subscriber pursuant to Section 3.3 provisions.

3.3.2 Identification and Authentication of Re-key After Certificate Revocation

Subscriber shall repeat the Section 3.2 “Initial Registration” procedures upon the

application for issuance of new certificate after the certificate is revoked.

3.3.3 Re-key After Certificate Renewal

Certification Authority may, depending on the demand, decide whether or not it will provide certificate renewal service. If the Certification Authority provides certificate renewal service, the following provisions shall be observed:

(1) The Certification Authority's certificate is not subject for renewal.

(2) All certificate renewal operations, except the revoked subscriber's certificate, can be provided pursuant to the Certification Authority's requirements without re-key.

3.4 Identification and Authentication of Certificate Revocation Application

(1) Certification Authority or Registration Authority shall authenticate the certificate revocation application pursuant to Section 4.9 "Temporary Suspension and Revocation of the Certificate" provisions.

(2) Certification Authority shall, in the Certification Practice Statement, specify the means of authenticating applicant identity.

4 Operational Requirements in a Certificate Lifespan

4.1 Certificate Application

4.1.1 Certificate Applicant

Certificate applicants include:

(1) Subordinate Certification Authority;

(2) Certificate applicant, include organization or individual, of the subordinate Certification Authority.

4.1.2 Registration Procedures and Responsibility

Certification Authority shall, in the Certification Practice Statement, specify the identification and authentication of certificate applicant identity and the obligations of the subscriber of the certificate.

4.2 Certificate Application Procedures

(1) The Root Certification Authority shall, in the Certification Practice Statement, specify the subordinate Certification Authority's application procedures.

(2) Subordinate Certification Authority's certificate application shall be approved by its superior Certification Authority.

(3) Certification Authority shall, in the Certification Practice Statement, specify the initial registration procedures, certificate renewal procedures, certificate re-key procedures, and application location or URL.

(4) The procedures for cross-certificate application between non-GPKI Certification Authority and the Root Certification Authority shall be enacted by NDC separately.

4.2.1 Performance of Identification and Authentication Functions

The Issuing Certification Authority shall ensure the system and procedures are sufficient to authenticate the subscriber's identity pursuant to Section 3.2 "Initial Registration" provisions herein.

The Issuing Certification Authority of SSL certificate shall specify in the Certification Practice Statement regarding the procedures to authorize the Issuing Certification Authority to review and confirm the domain name system resource record.

4.2.2 Approval or Refusal of Certificate Application

The certificate application can be accepted upon the Issuing Certification Authority's completion of identity authentication.

Certification Authority can refuse to issue certificate under the following circumstances:

(1) When the identity authentication failed to pass;

(2) Other reasons identified by the Certification Authority.

4.2.3 Processing Time for Certificate Application

Certification Authority and Registration Authority shall specify in the Certification Practice Statement regarding the time required to complete the certificate application process.

4.3 Certificate Issuance Procedures

4.3.1 Operation of Certification Authority

Certification Authority's issuance of certificate shall, pursuant to provisions of Section 5.2 "Procedural Controls" herein and the Certification Practice Statement, be performed by adequate personnel, and the Certification Authority or Registration Authority shall notify the applicant via appropriate means.

4.3.2 Certification Authority's Notification to the Certificate Applicant

Certification Authority operate with AL 1 assurance level or above shall specify the following particulars in the Certification Practice Statement:

(1) The means of notifying the applicant when it agrees to issue the certificate.

(2) The means of notifying the applicant when it refuses to issue the certificate.

4.4 Certificate Acceptance Procedures

Certification Authority operate with AL 2 assurance level or above shall publish the certificate in the repository after the certificate applicant reviewed the certificate contents and accepted the certificate. If the certificate applicant refuses to accept the certificate, Certification Authority shall revocation the certificate.

Certification Authority operate with AL 2 assurance level or above shall specify the following particulars in the Certification Practice Statement:

(1) The certificate applicant's means to accept or refuse the certificate.

(2) The certificate field, which shall include at least name of the subject, that the certificate applicant shall review before accepting the certificate.

(3) The subsequent processing method when the certificate applicant refuses to accept the certificate.

The Root Certification Authority shall, in the Certification Practice Statement, specify the procedures of accepting the self-signed certificate and self-issued certificate.

4.4.1 Elements of Certificate Acceptance

The certificate applicant shall, upon receiving the certificate, confirm accuracy of the certificate contents and acknowledgement of provisions relating to the use of the certificate prior to using the certificate.

4.4.2 Certificate Published by Certification Authority

Certification Authority shall publish the issued certificate in the repository

periodically

Certification Authority may commission Registration Authority or other organizations to transmit the certificate to its subscriber.

4.4.3 Certification Authority's Certificate Issuance Notification to Other Entities

Certification Authority may, at its own discretion, determine whether it will notify other entities regarding the issuance of the certificate. The Certificate Policy will not specify in this regard.

4.5 Usage of the Key Pair and Certificate

4.5.1 Subscriber's Use of Private Key and Certificate

(1) The generation of key pair shall comply with Section 6.1.1 "Key Pair Generation", and the subscribers shall have the right to control the private key.

(2) Private key shall not be used on certificate issuance.

(3) Private key shall be protected against unauthorized use or disclosure by others.

(4) Ensure that the private key is used pursuant to the key usage noted in the extension fields of the certificate.

(5) The certificate shall be used pursuant to the Certificate Policy stated on the certificate.

4.5.2 Relying Party's Use of Public Key and Certificate

(1) Relying party shall comply with the Certification Practice Statement provisions of each Certification Authority when using the certificate.

(2) The certificate shall be proven validity before applying in the following operations:

- To verify the integrity of electronic document's digital signature.
- To verify identity of the signatory of the document.
- To establish secure communication channel with the subscribers.

(3) Each Certification Authority shall, in the Certification Practice Statement, specify the means to verify the certificate.

4.6 Certificate Renewal

If the Certification Authority provides certificate renewal service, the following provisions shall be observed:

(1) The Certification Authority's certificate is not subject for renewal.

(2) All certificate renewal operations, except the revoked subscriber's certificate, can be provided pursuant to the Certification Authority's requirements.

(3) The renewal period of subscriber's certificate shall be processed pursuant to Section 6.3.2.2 "Usage Period of the Subscriber's Public Key and Private Key" provisions.

4.6.1 Causes of Certificate Renewal

Each Certification Authority shall, in the Certification Practice Statement, specify whether it provides certificate renewal service or not.

4.6.2 Applicant of Certificate Renewal

If the Certification Authority provides certificate renewal service, it shall specify in the Certification Practice Statement regarding the qualifications of the certificate renewal applicant. If the applicant is not qualified, the Certification Authority shall inform the disqualification reason.

4.6.3 Certificate Renewal Procedures

If the Certification Authority provides certificate renewal service, it shall specify in the Certification Practice Statement regarding the procedures of certificate renewal.

4.6.4 Notification for the Issuance of Renewed Certificate to the Subscribers

Certification Authority shall, upon completion of the subscriber's certificate renewal, notify the subscriber pursuant to Section 4.3.2 "Certification Authority's Notification to the Certificate Applicant" provisions. If the Certification Authority disapprove the renewal or the certificate cannot be renewed, it shall clearly inform the reason for not being able to renew the certificate in question.

4.6.5 Elements for the Acceptance of Renewed Certificate

The certificate applicant shall, upon receiving the renewed certificate, confirm accuracy of the certificate contents prior to using the certificate.

4.6.6 Certification Authority's Publication of Renewed Certificate

Certification Authority shall publish the renewed certificate in the repository periodically.

Certification Authority may commission Registration Authority or other organizations to transmit the renewed certificate to its subscriber.

4.6.7 Certification Authority's Notification of Issuance of Renewed Certificate to Other Entities

Certification Authority may, at its own discretion, determine whether it will notify other entities regarding the issuance of the renewed certificate. The Certificate Policy will not specify in this regard.

4.7 Certificate's Re-key

4.7.1 Causes of CA Re-key

(1) Certification Authority shall replace the key pair pursuant to Section 6.3.2.1 "Usage Period of the CA Public Key and Private Key" provisions.

(2) Certification Authority shall, upon revocation of its own certificate, suspend the

use of its private key and replace the key pair.

4.7.2 Re-key Applicant

Re-key applicant shall be subscriber of the certificate or the representative authorized to act on behalf of the subscriber and responsible for safekeeping of the certificate's corresponding private key.

4.7.3 Re-key Procedures

Certification Authority shall reverify the the subscriber's identity and issued certificate pursuant to "Operational Requirements in a Certificate Lifespan" herein. Certification Authority may request the certificate applicant to provide additional information in order to verify the subscriber's identity.

4.7.4 Notification of Issuance of Changed Key to the Subscriber

Certification Authority shall, upon completion of re-key for the subscriber's certificate, notify the subscriber pursuant to Section 4.3.2 "Certification Authority's Notification to the Certificate Applicant" provisions. If the Certification Authority disapprove the re-key or the subscriber's certificate cannot be re-keyed, it shall clearly inform the reason for not being able to re-key the subscriber's certificate.

4.7.5 Elements for the Acceptance of Changed Key

The certificate applicant shall, upon receiving the renewed certificate, confirm accuracy of the certificate contents prior to using the certificate.

4.7.6 Certification Authority's Publication of the Changed Key

Certification Authority shall publish the re-keyed certificate in the repository periodically.

Certification Authority may commission Registration Authority or other organizations to transmit the re-keyed certificate to its subscriber.

4.7.7 Certification Authority's Certificate Issuance Notification to Other Entities

Certification Authority may, at its own discretion, determine whether it will notify other entities regarding the issuance of the certificate. The Certificate Policy will not specify in this regard.

4.8 Certificate Modification

4.8.1 Causes of Certificate Modification

Certification Authority shall, in the Certification Practice Statement, specify causes of certificate modification.

4.8.2 Applicant of Certificate Modification

Re-key applicant shall be subscriber of the certificate or the representative authorized to act on behalf of the subscriber and responsible for safekeeping of the

certificate's corresponding private key.

4.8.3 Certificate Modification Procedures

Certificate modification procedures shall be performed pursuant to Section 4.2 "Certificate Application Procedures" provisions.

4.8.4 Notification of Issuance of modified certificate to the Subscriber

Certification Authority shall, upon completion of modification for the subscriber's certificate, notify the subscriber pursuant to Section 4.3.2 "Certification Authority's Notification to the Certificate Applicant" provisions. If the Certification Authority disapprove the modification or the certificate cannot be modified, it shall clearly inform the reason for not being able to modify the certificate in question.

4.8.5 Elements for the Acceptance of Modified Certificate

The certificate applicant shall, upon receiving the renewed certificate, confirm accuracy of the certificate contents prior to using the certificate.

4.8.6 Certification Authority's Publication of the Modified Certificate

Certification Authority shall publish the modified certificate in the repository periodically.

Certification Authority may commission Registration Authority or other organizations to transmit the modified certificate to its subscriber.

4.8.7 Certification Authority's Certificate Issuance Notification to Other Entities

Certification Authority may, at its own discretion, determine whether it will notify other entities regarding the issuance of the certificate. The Certificate Policy will not specify in this regard.

4.9 Temporary Suspension and Revocation of the Certificate

(1) Certification Authority operate with AL 1 assurance level or above shall all provided certificate revocation service and may determine at its own discretion whether it will provide temporary suspension service for the certificate.

(2) If the Certification Authority provides certificate revocation service:

- It shall specify in the Certification Practice Statement regarding service time of the certificate revocation service, means of providing the service, certificate revocation application procedures, and application location or URL. If it also provides temporary certificate suspension (reuse) service, it shall also specify the aforesaid information in the Certification Practice Statement.
- The revoked and suspended certificates shall be listed on the Certification Authority Revocation List or Certificate Revocation List before the next scheduled publication of the Certification Authority Revocation List or

Certificate Revocation List and announced in the repository until the certificates are expired or reused; the certificate status announcement shall include the revoked and suspended certificates.

4.9.1 Causes of Certificate Revocation

Certification Authority shall, in the Certification Practice Statement, specify the causes of certificate revocation, which shall include at least the following causes:

(1) When the private key is lost, proven or suspected of being compromised.

(2) Modification on the subject information listed on the certificate shall be determined by the Certification Authority after assessment

4.9.2 Certificate Revocation Applicant

Certificate revocation applicant include at least the following:

(1) Certification Authority;

(2) "Subscribers" defined in Section 1.3.4.

4.9.3 Certificate Revocation Procedures

Certification Authority or Registration Authority shall, upon the completion of identity identification and authentication pursuant to Section 3.4 "Identification and Authentication of Certificate Revocation Application" herein, grant the certificate revocation application.

If the Certification Authority's key is proven compromised, the Certification Authority's certificate and its issued certificate shall be revoked immediately without the need to carry out identification and authentication process.

Certification Authority operate with AL 1 assurance level or above shall specify in the Certification Practice Statement regarding means of notifying the revoked certificate.

4.9.4 Grace Period for the Certificate Revocation Application

Certification Authority shall, if certificates were revoked due to suspected or confirmed key compromise or other security causes, report to the superior Certification Authority within 1hr.

Subscriber shall, if its certificate shall be revoked due to suspected or confirmed key compromise or other security causes, submit certificate revocation application at the earliest convenience.

4.9.5 Certification Authority's Processing Period for the Certificate Revocation Application

Certification Authority shall, in the Certification Practice Statement, specify the processing period of certificate revocation application.

4.9.6 Requirement for the Relying Party to Check the Revoked Certificate

Relying party using certificate with AL 2 level of assurance or above shall, prior to the use of the certificate, enquire current Certification Authority Revocation List and Certificate Revocation List or check the certificate via Online Certificate Status Protocol's enquiry service.

Relying party shall, take into consideration the risks, responsibility and affect and upon its own discretion, determine the time to obtain the certificate revocation information.

Certification Authority shall, in the Certification Practice Statement, specify the relying party's request to check the Certification Authority Revocation List or the Certificate Revocation List.

4.9.7 Frequency of Issuance of Certification Authority Revocation List and Certificate Revocation List

The Certification Authority Revocation List or Certificate Revocation List shall be published periodically, even when there is no change on the status of the certificate, to ensure instantaneity of the certificate status information.

The frequency of the issuance of Certification Authority Revocation List and Certificate Revocation List are shown in Schedule 4-1:

Schedule 4-1 Frequency of Issuance of Certification Authority Revocation List and Certificate Revocation List

issuance frequency / assurance level	Certification Authority Revocation List	Certificate Revocation List
test level	Certification Authority may formulate its own list as needed	Certification Authority may formulate its own list as needed
AL 1	Certification Authority may formulate its own list as needed	Certification Authority may formulate its own list as needed
AL 2	Certification Authority may formulate its own list as needed	at least once every 3 days
AL 3	at least once a day	at least once a day
AL 4	at least once a day	at least once a day

4.9.8 Maximum Latency in the Publication of the Certification Authority Revocation list and Certificate Revocation List

Certification Authority shall publish the Certification Authority Revocation List or Certificate Revocation List before the publication time shown in the "next update" field

on the Certification Authority Revocation List or Certificate Revocation List.

4.9.9 Online Certificate Revocation and Status-Checking Services

Certification Authority shall provide Certification Authority Revocation List or Certificate Revocation List and check status of the certificate. Certification Authority shall, in the Certification Practice Statement, specify whether it provides the Online Certificate Status Protocol enquiry service or not.

4.9.10 Provisions Regarding Double-Checking the Revoked Certificate Online

Certification Authority shall, in the Certification Practice Statement, specify the means for the relying party to check the revoke certificate online.

4.9.11 Other Forms of Revocation Announcement

Certification Authority may provide other form of revocation announcement due to operational considerations. The Certificate Policy will not specify in this regard.

4.9.12 Other Special Provisions on Compromised Key

Certification Authority shall, when the key is compromised, specify any other special provision in the Certification Practice Statement.

4.9.13 Causes of Temporary Suspension and Reuse of a Certificate

Each Certification Authority shall, in the Certification Practice Statement, specify whether it will provide temporary suspension and reuse services for the certificate or not.

4.9.14 Applicant of Temporary Suspension and recovery of a certificate

The applicant shall be subscriber of the certificate or the representative authorized to act on behalf of the subscriber and responsible for safekeeping of the certificate's corresponding private key.

4.9.15 Procedures of Temporary Suspension and Reuse of a Certificate

Certification Authority shall, in the Certification Practice Statement, specify the procedures of temporary suspension and reuse of a certificate.

4.9.16 Constraints During Temporary Suspension of the Certificate

Certification Authority shall, in the Certification Practice Statement, specify the constraints during the processing period of temporary suspension of certificate.

4.10c Ertificate Status Services

4.10.1 Service Features

Certification Authority shall provide Certification Authority Revocation List or Certificate Revocation List, Online Certificate Status Protocol enquiry service, or certificate status enquiry service provided by both lists.

4.10.2 Service Availability

Certification Authority shall provide 7 x 24hrs certificate status enquiry services.

4.10.3 Optional Features

Certification Authority may, at its own discretion, determine optional features of the certificate status services. The Certificate Policy will not specify in this regard.

4.11 Termination of Services

Certification Authority shall, when the subscriber no longer uses the Certification Authority's service, allow the subscriber to terminate the service.

4.12 Escrow and Recovery of Private Key

4.12.1 Policy and Practices for Key Escrow and Recovery

The signing private key is not allowed to be escrowed at the Certification Authority.

4.12.2 Key Encapsulation and Recovery Policy and Practices for Communication

Certification Authority shall, if it supports the encapsulation and recovery of communication key, specify the practice in the Certification Practice Statement.

5 Infrastructures, Security Management and Operation Procedures Controls

Unless otherwised specified, this chapter is applicable to the Certification Authority operates with AL 2 level of assurance or above.

5.1 Physical Control

5.1.1 Physical Location and Structure

The physical location and structure of the machine room shall prevent unauthorized access by a combination of physical security mechanisms such as access control, security, intrusion detection, surveillance video, etc.

5.1.2 Physical Access

(1) The physical control provisions for the Certification Authority operates with AL 2 level of assurance are as follows:

- Shall prevent unauthorized intrusion.
- The storage media and documents with sensitive information shall be stored in secure premises.

(2) The physical control provisions for the Certification Authority operates with AL 3 or AL 4 level of assurance are as follows:

- Shall set up 24-hour manual or electronic monitoring equipment.
- Shall maintain and review access log periodically.
- There shall be at least 2 persons jointly perform the physical control over the computer system and cryptographic module.

5.1.3 Electrical Power and Air Conditioning

Certification Authority shall be equipped with adequate electrical power, air conditioning and UPS with at least 6hrs of backup power.

5.1.4 Flood Prevention and Protection

Selection of Certification Authority's setup site shall take into consideration of possible flood to avoid flood damage.

5.1.5 Fire Prevention and Protection

Certification Authority shall be equipped with automatic fire detection and activate fire extinguish functions.

5.1.6 Media Storage

Certification Authority shall protect relevant storage media from accidental damage.

5.1.7 Waste Disposal

Certification Authority may specify its own waste disposal methods. The Certificate Policy will not specify in this regard.

5.1.8 Remote Backup

Certification Authority shall carry out related system remote backup operation periodically and specify the backup, backup cycle and backup location in the Certification Practice Statement.

The remote backup system shall be equipped with the same security level as that of the official system.

5.2 Procedural Controls

5.2.1 Trusted Roles

Certification Authority shall, take into consideration the security and validity of the certificates, provide trusted roles to perform related tasks and adequately separate various tasks with at least 2 persons deployed on the same task.

Certification Authority shall, in the Certification Practice Statement, specify the definition of the trusted roles.

5.2.2 Number of People Required for an Individual Task

The performance of an individual task shall not be completed by a single staff. Certification Authority shall, in the Certification Practice Statement, specify the task of the trusted roles and number of people deployed to each task.

5.2.3 Identification and Authentication of Each Role

The trusted roles shall undergo identity identification and authentication operations before performing tasks.

5.2.4 Division of the Authority and Responsibility of Each Role

Certification Authority shall, in the Certification Practice Statement, specify the division of authority and responsibility of the trusted roles.

5.3 Personnel Controls

Certification Authority shall possess control over its certificate operations related personnel.

5.3.1 Background, Qualifications, Experiences and Security Cearance Requirements

Certification Authority shall undergo the identification operation on its operation related personnel and specify the qualifications, selection, supervision and auditing methods of personnel in the Certification Practice Statement.

5.3.2 Background Check Procedures

Certification Authority shall, in the Certification Practice Statement, specify the operational personnel background check procedures.

5.3.3 Training Requirements

CA personnel shall be subject to related trainings, which include at least the following contents:

(1) Certification Authority's security certification mechanism;

(2) Software and hardware used in the Certification Authority's system;

(3) Job assignments;

(4) Post-disaster recovery and business continuity plan.

5.3.4 Personnel Retraining Requirements and Frequency

Certification Authority shall undergo personnel retraining when there are major changes such as changes in laws and regulations, software and hardware upgrades or changes in work procedures and specify the requirements and frequency in the Certification Practice Statement.

5.3.5 Job Rotation Frequency and Sequence

Certification Authority may define job rotation frequency and sequence pursuant to the Statement. The Certificate Policy will not specify in this regard.

5.3.6 Sanctions for Unauthorized Actions

Certification Authority shall, in the Certification Practice Statement, specify the means of sanctions upon personnel's violation of the provisions.

5.3.7 Provisions on Contract Personnel

Certification Authority shall, in the Certification Practice Statement, specify the provisions on hiring personnel to serve at relevant function of the Certification Authority.

5.3.8 Documentation Provided to Personnel

Certification Authority shall, in the Certification Practice Statement, specify the provision of documentations required for the relevant CA personnel to perform their business.

5.4 Procedures on Logging of Audit Trail

Certification Authority operates with AL 1 level of assurance or above shall be equipped with adequate audit logging function. Certification Authority shall, in the Certification Practice Statement, specify audit logginging procedures.

5.4.1 Type of Log

Certification Authority shall record at least the following audit trail particulars:

(1) Type of event;

(2) Event-causing entity or event manipulator;

(3) Event occurance site or location;

(4) Event occurance date and time;

(5) Records of successful (or unsuccessful) certificate issuance or revocation operations.

The audit trails that the Certification Authority shall record are shown in Schedule 5-1.

Schedule 5-1 Provisions on the Logging of Audit Trails

auditable trail / assurance level	AL 1	AL 2	AL 3	AL 4
A.1 Security Audit				
A.1.1 Important changes in audit parameters, such as audit frequency, type of audit event and contents of the new / old parameters.		✓	✓	✓
A.1.2 Attempted deletion or revision on audit log		✓	✓	✓
A.2 Identification and Authentication				
A.2.1 Successful and unsuccessful attempts to assume a role		✓	✓	✓
A.2.2 Changes in the number of maximum identification or authorization attempts		✓	✓	✓
A.2.3 Maximum number of unsuccessful identification or authorization attempts during subscriber login		✓	✓	✓
A.2.4 Administrator unlocks an account that has been locked as a result of unsuccessful identification or authorization attempts		✓	✓	✓
A.2.5 Administrator changes identity authentication mechanism of the system, such as changing from passwords to biometric value		✓	✓	✓
A.3 Generation of Key				
A.3.1 Times when a key is generated by Certification Authority	✓	✓	✓	✓
A.4 Upload and Storage of Private Key				
A.4.1 Uploading of private keys into system components	✓	✓	✓	✓
A.4.2 Any access to the Subject's private keys for key recovery purposes	✓	✓	✓	✓
A.5 Additions, Deletions and Storage of Trusted Public Key				
A.5.1 Changes to the additions, deletions and storage of trusted public key	✓	✓	✓	✓
A.6 Export of Private Key				
A.6.1 Export of private key, except for one-time use keys	✓	✓	✓	✓
A.7 Certificate Registration				
A.7.1 Processes of certificate registration application	✓	✓	✓	✓
A.8 Certificate Revocation				
A.8.1 Processes of certificate revocation		✓	✓	✓
A.9 Certificate Status Change Approval				
A.9.1 Approval or refusal on certificate status change applocation		✓	✓	✓

auditable trail / assurance level	AL 1	AL 2	AL 3	AL 4
A.10 Configuration Setting of GRCA or Subordinate CA				
A.10.1 Changes to configuration setting related to CA security		✓	✓	✓
A.11 Account Management				
A.11.1 Addition or deletion on the roles or subscribers	✓	✓	✓	✓
A.11.2 Revision on the access authorization of a subscriber account or role	✓	✓	✓	✓
A.12 Certificate Profile Management				
A.12.1 Certificate profile changes	✓	✓	✓	✓
A.13 CARL / CRL profile management				
A.13.1 CARL / CRL profile modifications		✓	✓	✓
A.14 Miscellaneous				
A.14.1 Installation of operating system		✓	✓	✓
A.14.2 Installation of CA system		✓	✓	✓
A.14.3 Installation of hardware cryptographic modules			✓	✓
A.14.4 Removal of hardware cryptographic modules			✓	✓
A.14.5 Destruction of hardware cryptographic modules		✓	✓	✓
A.14.6 System activation		✓	✓	✓
A.14.7 Login attempts to CA apps		✓	✓	✓
A.14.8 Receipt of hardware / software			✓	✓
A.14.9 Attempts to create passwords		✓	✓	✓
A.14.10 Attempts to change passwords		✓	✓	✓
A.14.11 CA internal database backup		✓	✓	✓
A.14.12 CA internal database recovery		✓	✓	✓
A.14.13 Creating, naming and transferring of file			✓	✓
A.14.14 Transmission of any information to repository			✓	✓
A.14.15 Access to the CA internal database			✓	✓
A.14.16 Any certificate compromise complaint		✓	✓	✓
A.14.17 Certificate uploaded tokens			✓	✓
A.14.18 Token transmission process			✓	✓
A.14.19 Token zeroization		✓	✓	✓
A.14.20 CA Re-key	✓	✓	✓	✓
A.15 Configuration Changes to the CA Server				
A.15.1 Hardware		✓	✓	✓
A.15.2 Software		✓	✓	✓
A.15.3 Operating system		✓	✓	✓
A.15.4 Patches		✓	✓	✓
A.15.5 Security profiles			✓	✓
A.16 Physical Access and Site Security				
A.16.1 Physical access to the CA machine room			✓	✓
A.16.2 Access to CA servers			✓	✓
A.16.3 Known or suspected violations of physical security regulations		✓	✓	✓
A.17 Abnormalities				
A.17.1 Software error		✓	✓	✓
A.17.2 Unsuccessful software integrity check		✓	✓	✓

auditable trail / assurance level	AL 1	AL 2	AL 3	AL 4
A.17.3 Receipt of improper messages			✓	✓
A.17.4 Misrouted messages			✓	✓
A.17.5 Network attack		✓	✓	✓
A.17.6 Equipment failure	✓	✓	✓	✓
A.17.7 Improper power supply			✓	✓
A.17.8 UPS failure			✓	✓
A.17.9 Noticeable or significant network service or access failures			✓	✓
A.17.10 Violations of Certificate Policy	✓	✓	✓	✓
A.17.11 Violations of the Certification Practice Statement	✓	✓	✓	✓
A.17.12 Resetting of the operating system clock		✓	✓	✓

5.4.2 Frequency of Log Processing

Certification Authority shall, in the Certification Practice Statement, specify the frequency of log processing pursuant to Schedule 5-2 provisions.

Schedule 5-2 Frequency of Log Processing

assurance level	frequency of log processing
AL 2	Certification Authority may, at its own discretion, determine the frequency of log processing. The Certificate Policy will not specify in this regard.
AL 3	Certification Authority shall, at least once every two months, review major security audit logs occurred since last audit review and further investigate any possible malicious activities.
AL 4	Certification Authority shall, at least once every month, review major security audit logs occurred since last audit review and further investigate any possible malicious activities.

5.4.3 Audit Log Retention Period

CA audit log shall be kept in-situ for at least 2 months and processes pursuant to Section 5.4.4, 5.4.5, 5.4.6 and 5.5 provisions.

The audit logs shall, upon expiration of the retention period, be removed by auditor instead of any other personnel.

5.4.4 Audit Log Protection

Certification Authority shall take adequate mechanism to protect the audit logs in order to avoid unauthorized access.

Certification Authority shall, in the Certification Practice Statement, specify audit log protection method.

5.4.5 Audit Log Backup Procedures

Certification Authority shall, in the Certification Practice Statement, specify audit log backup practice pursuant to Schedule 5-3 provisions.

Schedule 5-3 Audit Log Backup Procedures

assurance level	audit log backup procedures
AL 2	Local backup at least once a month.
AL 3	
AL 4	Local and remote backup at least once a month.

5.4.6 Audit Log Compaction System

The audit system shall continue operation since the activation of certificate system until the certificate management system is turned off.

5.4.7 Informing the Person Who Caused the Event

The audit system does not need to inform the entity causing the event.

5.4.8 Vulnerability Assessment

Certification Authority operates with AL 3 and AL 4 level of assurance shall periodically perform vulnerability assessment.

5.5 Log Archiving Methods

5.5.1 Type of Archived Logs

The logs that the Certification Authority shall archive are shown in Schedule 5-4.

Schedule 5-4 Archiving Records

archiving log / assurance level	AL 1	AL 2	AL 3	AL 4
CA accreditation (by the competent authority) process and result information	✓	✓	✓	✓
Certification Practice Statement	✓	✓	✓	✓
Major contracts	✓	✓	✓	✓
System and equipment configuration settings	✓	✓	✓	✓
Modifications and updates to systems or configuration settings	✓	✓	✓	✓
Certificate application information	✓	✓	✓	✓
Revocation application information		✓	✓	✓
Subscriber's identity identification information		✓	✓	✓
Document receipt and certificate acceptance		✓	✓	✓
Token activation log		✓	✓	✓
Issued or published certificates	✓	✓	✓	✓
CA rekey records	✓	✓	✓	✓
Issued and/or published CARLs / CRLs		✓	✓	✓
Audit logs	✓	✓	✓	✓

archiving log / assurance level	AL 1	AL 2	AL 3	AL 4
Other information or applications used to verify or substantiate archive contents		✓	✓	✓
Document required by the auditors		✓	✓	✓

5.5.2 Retention Period of Archived Logs

The retention period of archived logs shall, except for the test level, not be less than the issued duration.

Certification Authority shall, in the Certification Practice Statement, specify the method of processing the archived logs upon the expiration of retention period of archives.

5.5.3 Protection of Archived Logs

(1) The archived logs shall not be changed or deleted;

(2) The archived logs shall be stored at the location equipped with security control measures and harmless to the storage media.

(3) The archived logs may be provided to other individual or organization upon the subscriber's authorization and consent.

5.5.4 Backup Procedures for Archived Logs

Certification Authority may, at its own discretion, determine backup procedures for the archived logs based on its needs. The Certificate Policy will not specify in this regard.

5.5.5 Time-Stamping Requirements for the Archived Logs

Certification Authority may, at its own discretion, determine the time-stamping requirements for the archived logs based on its needs. The Certificate Policy will not specify in this regard.

5.5.6 Compaction System for the Archived Logs

Certification Authority may, at its own discretion, determine the compaction system for the archived logs based on its needs. The Certificate Policy will not specify in this regard.

5.5.7 Procedures on Obtaining and Verifying the Archived Logs

Certification Authority shall, in the Certification Practice Statement, specify the procedures on obtaining and verifying the archived logs.

5.6 Re-key

5.6.1 CA Re-key

(1) Certification Authority shall, pursuant to Section 6.3.2 "Usage Period of the Subscriber's Public Key and Private Key" provisions, replacement private key periodically and make announcement.

(2) Old private key shall still be used to issue response message of the Certification

Authority Revocation List, Certificate Revocation List or Online Certificate Status Protocol and maintained until all of the subscriber's certificate issued by old private key are expired.

(3) Certification Authority shall, if its own certificate is revoked, suspend its private key and replace the key pair.

(4) The Root Certification Authority shall, 3 months before the self-signed certificate expires, replace the key pair used for the issuance of subordinate CA's certificate, issue 1 new self-signed certificate, and use new / old private key to issue 1 self-issued certificate to each other. The new certificate issuance procedures are subject to Section 4.3 "Certificate Issuance Procedures" provisions.

(5) Subordinate Certification Authority shall, 2 months before the certificate expires, replace the key pair used for the issuance of certificate. The subordinate Certification Authority shall, after replaced the key pair, apply for new certificate pursuant to Section 4.2 "Certificate Application Procedures" provisions.

5.6.2 Subscriber's Re-key

(1) Subscriber's private key shall be replaced periodically pursuant to Section 6.3.2 "Usage Periods of the Public Key and Private Key" provisions.

(2) The subscriber shall, upon certificate revocation, suspend the use of its private key. If new certificate application is required, it shall be processed pursuant to Section 4.2 "Certificate Application Procedures" provisions.

(3) Certification Authority shall, in the Certification Practice Statement, specify the subscriber's re-key provisions.

5.7 Recovery Procedures When the Key is Compromised or Following A Disaster

Certification Authority's post-disaster recovery job shall be performed by recovering the repository first in order to provide certificate status information as usual.

5.7.1 Processing Procedures for Emergency and Compromised System

Certification Authority shall, in the Certification Practice Statement, specify the notifications, processing, and recovery procedures, which shall carry out exercise operation every year, for an emergency or when the system is compromised.

5.7.2 Recovery Procedures for Compromised Computer Resources, Software or Data

Certification Authority shall, in the Certification Practice Statement, specify the recovery procedures for compromised computer resources, software or information.

Certification Authority operates with AL 3 and AL 4 level of assurance shall carry out exercise operation at least once a year.

5.7.3 Recovery Procedures for Compromised CA Signing Key

Certification Authority shall, in the Certification Practice Statement, specify the recovery procedures for compromised CA signing key.

Certification Authority operates with AL 3 and AL 4 level of assurance shall carry out exercise operation at least once a year.

5.7.4 Certification Authority's Post-Disaster On-Going Operation

Certification Authority shall, in the Certification Practice Statement, specify Certification Authority's post-disaster on-going operation.

Certification Authority operates with AL 3 and AL 4 level of assurance shall carry out exercise operation at least once a year.

5.7.5 Recovery Procedures for Certification Authority's Revoked Signing-Key Certificate

Certification Authority shall, in the Certification Practice Statement, specify the recovery procedures for Certification Authority's revoked signing-key certificate.

Certification Authority operates with AL 3 and AL 4 level of assurance shall carry out exercise operation at least once a year.

5.8 Termination of CA or RA Services

Termination of CA or RA services shall be handled pursuant to the relevant provisions of the Electronic Signatures Act.

6 Technical Security Control

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

(1) The cryptographic module used by the Certification Authority in certificate issuance shall comply with FIPS 140-2 specifications or receive consent of the Root Certification Authority.

(2) The generated private key shall be protected against access by non-authorized personnel or under unrecorded circumstances.

(3) Certification Authority shall take adequate measures to ensure the uniqueness of the subscriber's public key.

(4) The entity that generated signing private key on behalf of the subscribers shall not retention backup of that key.

(5) For the Certification Authority operates with AL 4 level of assurance, the subscriber's random number, key pair and symmetric key shall not be generated by hardware.

6.1.2 Secure Delivery of Private Keys to Subscribers

(1) The key-generating entity shall, in addition to the generation of private key and the storage of private key in subscriber's cryptographic module, deliver the private key to the Subject via secure and auditable means.

(2) Certification Authority shall, in the Certification Practice Statement, specify the means of secure delivery of private key to the subscriber and the subscriber's means of confirming the acceptance of the private key.

6.1.3 Secure Delivery of Public Keys to the CA

Certification Authority shall, in the Certification Practice Statement, specify the means of secure delivery of public key to the Certification Authority.

6.1.4 Secure Delivery of CA Public Keys to Relying Parties

Certification Authority shall, in the Certification Practice Statement, specify the means of secure delivery of CA public key to the relying party.

6.1.5 Key Sizes

The certificate shall use 2048-bit (or higher) RSA key or other type of key with an equivalent security strength.

The response message of the certificate, Certification Authority Revocation List, Certificate Revocation List and Online Certificate Status Protocol shall use SHA-2 algorithm or algorithm with an equivalent security strength.

6.1.6 Generation and Quality Check of the Public Key Parameters

The public key parameters shall comply with international standard and be subject to the primality test.

Certification Authority shall, in the Certification Practice Statement, specify the primality test methodogy.

6.1.7 Usage Purposes of Key

The certificate's public key shall, pursuant to X.509 standard, specify its usage in the "key usage" extension field on the certificate.

Certification Authority shall, in the Certification Practice Statement, specify the usage purposes of key.

6.2 Private Key Protection and Security Control Measures for the Cryptographic Module

6.2.1 Standards and Control of Cryptographic Module

The cryptographic module shall comply with FIPS 140-2 standard or other standard with an equivalent security strength, and it shall at least comply with Schedule 6-1 "Cryptographic Module Standard Provisions".

Schedule 6-1 Cryptographic Module Standard Provisions

assurance level	Root Certification Authority	Subordinate Certification Authority	Registration Authority	Subscribers
test level	N/A	in discretion	in discretion	in discretion
AL 1	N/A	AL 1	AL 1	in discretion
AL 2	N/A	AL 2	AL 1	AL 1
AL 3	N/A	AL 2	AL 2	AL 1
AL 4	AL 3	AL 3	AL 2	AL 2

※This Schedule referred to FIPS 140-2 standard

6.2.2 Multi-Person Control Over the Key

For the Certification Authority operates with AL 3 or AL 4 level of assurance, its signing private key shall be subject to the principle of multi-person control.

Certification Authority shall, in the Certification Practice Statement, specify the procedures of multi-person control over the key.

6.2.3 Escrow of Private Key

The signing private key shall not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of the Certification Authority's Signing Private Key

For the Certification Authority operate with AL 3 assurance level or above, its signing private key shall be backed up under multi-person control

procedures and stored in a secure premise.

Certification Authority shall, in the Certification Practice Statement, specify the procedures of backing up keys.

6.2.4.2 Backup of the Subscriber's Signing Private Key

Subscribers of the certificate with AL 1 to AL 3 level of assurance can backup or copy its signing private key at its own discretion.

Subscriber of the certificate with AL 4 level of assurance shall not backup or copy its signing private key.

6.2.5 Archive of Private Key

The signing private key shall not be archived.

6.2.6 Transmission Between Private Key and Cryptographic Module

(1) Key generation is subject to Section 6.1.1 "Key Pair Generation" provisions.

(2) Certification Authority shall, except for backup-key recovery, re-key and cryptographic module replacement, not carry out transmiission between the private key and the cryptographic module.

(3) Transmission between Certification Authority's private key and the cryptographic module can be carry out by encryption or multi-person control method; it shall not exist outside the cryptographic module in plain text form. The private key shall be input into the cryptographic module pursuant to Section 6.2.2 "Multi-Person Control Over the Key" provisions.

(4) Certification Authority shall, upon the completion of private key input, completely destroy the parameters generated during the process.

6.2.7 Storage of Private Key in Cryptographic Module

The private key shall be stored in the cryptographic module pursuant to the aforesaid provisions. The Certification Authority shall, if the cryptographic module no longer need to be used, turn it offline and store it in a secure premise.

6.2.8 Method of Activating Private Key

Before activating the private key in the cryptographic module, identity authentication on the activator shall be carried out and ensure information security; the activated private key shall be subject to security control.

6.2.9 Method of Deactivating Private Key

Certification Authority's private key shall be suspended from operation when it no longer needs to be used; Certification Authority shall, in the Certification Practice Statement, specify method of deactivating the private key.

6.2.10 Method of Destroying Private Key

When the Certification Authority destroys the signing private key, it shall also destroy the backup. The means of destruction are as follows:

(1) Software cryptographic module: the data must be rewritten on the memory or storage media originally occupied by the signature private key.

(2) Hardware cryptographic module: hardware cryptographic module must be physically destroyed or perform zeroization.

6.2.11 Cryptographic Module Rating

The level of cryptographic module is subject to Section 6.2.1 “standards and control of cryptographic module” provisions.

6.3 Other Provisions on Key Pair Management

The key pair shall not simultaneously be used on signature and encryption. Certification Authority shall, in the Certification Practice Statement, specify provisions on key pair management.

6.3.1 Archive of Public Key

The public key has already been archived at the time of archiving the certificate, therefore, there is no need to archive the public key again.

6.3.2 Usage Periods of the Public Key and Private Key

6.3.2.1 Usage Period of the CA Public Key and Private Key

(1) Lifespan of the signing private key used by the Root Certification Authority for signing the certificate shall not exceed half of the lifespan of the self-signed certificate;

(2) Sum of the lifespan of the certificate issued by the Root Certification Authority to the subordinate Certification Authority and the lifespan of signing private key used by the Root Certification Authority for signing the certificate shall not exceed the lifespan of the Root Certification Authority’s self-signed certificate;

(3) Lifespan of the self-issued certificate issued by the Root Certification Authority upon the replacement of its signing key shall not exceed duration of the old certificate;

(4) Usage periods of the CA public key and private key are as follows:

- RSA 4096-bit public key pair or other public key pair with an equivalent security strength: The maximum duration of the public key and private key are 30 years; if the private key is used on certificate issuance, its usage period shall not exceed 15 years.

- RSA 2048-bit public key pair or other public key pair with an equivalent security strength: The maximum duration of the public key and private key are 20 years; if the private key is used on certificate issuance, its usage period shall not exceed 10 years.

6.3.2.2 Usage Period of the Subscriber's Public Key and Private Key

Subscriber's key shall use at least 2048-bit RSA or other public key pair with an equivalent security strength; its private key usage period shall not exceed 10 years.

The 1024-bit RSA certificate issued by the Certification Authority can be no later than December 31, 2018.

6.4 Protection for the Activation Data

6.4.1 Generation of Activation Data

(1) For the Certification Authority operates with AL 1 to AL 3 level of assurance and its subscribers, its activation data may be chosen at the subscriber's own discretion.

(2) Certification Authority operates with AL 4 level of assurance and its subscribers shall adopt security mechanisms such as subscriber's biometric value or cryptographic module.

(3) Certification Authority shall, if password is used as the activation data, comply with the information security management guidelines and related information security requirements of the Executive Yuan and its affiliates.

6.4.2 Protection for the Activation Data

The activation data used for unlocking the private key shall be protected by adequate security mechanisms after assessment risks; the activation data shall be transmitted (if necessary) via adequate secure channel.

Certification Authority shall, in the Certification Practice Statement, specify protection mechanisms for the activation data.

6.4.3 Other Provisions for the Activation Data

Certification Authority may, at its own discretion, define other provisions for the activation data. The Certificate Policy will not specify in this regard.

6.5 Security Control Measures for the Computer Software and Hardware

6.5.1 Technical Requirements for the Security of Specific Computers

(1) Specific computer: referred to the private key storage equipment.

(2) The specific computer equipment shall be set on operating plaform that has passed the security assessment.

(3) For the Certification Authority operates with AL 3 level of assurance or above, its

technical requirements for the security of specific computers are as follows:

- Login via identity authentication;
- Shall define access control method;
- Providing security audit capacity;
- Ensuring the security upon every communication and the database;
- Being equipped with integrity and security control protection over the procedures.

6.5.2 Computer Security Rating

Certification Authority may, based on its needs, define the minimum standard of its computer secure rating. The Certificate Policy will not specify in this regard.

6.6 Lifespan Technical Control Measures

6.6.1 System Development Control Measures

Software used by the Certification Authority shall comply with system development control measures as follows.

Schedule 6-2 Provisions on System Development Control Measures

assurance level	system development control measures
test level	Certification Authority may decide at its own discretion. The Certificate Policy will not specify in this regard
AL 1	Certification Authority may decide at its own discretion. The Certificate Policy will not specify in this regard
AL 2 AL 3 AL 4	(1) Shall ensure that the software used was developed pursuant to the software engineering development method. (2) Hardware and software shall be dedicated and authorized. Software and hardware unrelated to operation shall not be installed. (3) Shall prevent unintended installation of malicious software. (4) Software shall be examined to see if there is any malicious code upon initial use, and it shall be scanned regularly.

6.6.2 Security Management Control Measures

Software used by the Certification Authority shall comply with security management measures as follows.

Schedule 6-3 Security Management Control Measures

assurance level	security management control measures
test level AL 1 AL 2	(1) Shall record and control related system configuration and system revision history; (2) Shall be equipped with mechanism capable of detecting unauthorized

assurance level	security management control measures
AL 3	revision on CA software or configuration; (3) Shall confirm if the software is the untempered correct version when installing the software.
AL 4	(1) Shall record and control related system configuration and system revision history; (2) Shall be equipped with mechanism capable of detecting unauthorized revision on CA software or configuration; (3) Shall confirm if the software is the untempered correct version when installing the software; (4) Shall verify the integrity of the CA software at least once a month.

6.6.3 Lifespan Security Control Measures

Certification Authority may, at its own discretion, determine the lifespan security control measures based on its needs. The Certificate Policy will not specify in this regard.

6.7 Network Security Control Measures

The Root Certification Authority shall not connect to any other host or external network other than the external repository host.

Certification Authority shall, in the Certification Practice Statement, specify network security control measures.

6.8 Time Stamps

Certification Authority may, at its own discretion, determine the related provisions for time-stamping based on its needs. The Certificate Policy will not specify in this regard.

6.9 Security Control Measures for the Cryptographic Module

The cryptographic module's security control measures method shall be subject to Section 6.1 "Key Pair Generation and Installation" and 6.2 "Private Key Protection and Security Control Measures for the Cryptographic Module" provisions.

7 Certificate, Certificate Revocation List and Online Certificate Status Protocol Profiles

7.1 Certificate Profile

7.1.1 Version Number

Certification Authority shall issuance X.509 v3 certificates.

7.1.2 Certificate Extension Fields

The certificate issued by Certification Authority operates with AL 3 level of assurance or above shall comply with the "Government Public Key Infrastructure Certificate and Certificate Revocation List Profile" provisions; Certification Authority operates with AL 1 or AL 2 level of assurance shall comply with provisions of the RFC 5280 standard.

The use of certificate's extension fields, processing methods, and setting of field values shallbe specified in the certificate profile..

If the Certification Authority needs to add new extension fields, the criticality to the new field shall be stated in the Certification Practice Statement.

7.1.3 Algorithm Object Identifier

The algorithm object identifiers used by Certification Authority upon certificate issuance are shown in the Schedule below:

Schedule 7-1 Algorithm Object Identifier

type	algorithm	algorithm Object Identifier
key generation	rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
signature	sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
	sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
	sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}

7.1.4 Name Forms

The subject and issuer's field values shall use X.500 distinguished name, and the attribute type of the name shall comply with RFC 5280 regulations.

7.1.5 Name Constraints

Certification Authority may, based on its needs, determine if the certificate shall use name constraints. The Certificate Policy will not specify in this regard.

7.1.6 Certificate Policy Object Identifier

Certificate shall record Certificate Policy Object Identifier. The Object Identifier

shall be consistent with the certificate's assurance level.

7.1.7 Policy Constraints on the Use of Extension Fields

Certification Authority may, based on its needs, determine if the certificate shall use "Policy Constraints" on extension fields. The Certificate Policy will not specify in this regard.

7.1.8 Syntax and Semantics of Policy Qualifier

Certificate shall not include "policy qualifier".

7.1.9 Semantic Processing for Critical Certificate Policy Extension Fields

The semantic processing for critical Certificate Policy extension fields shall comply with "Government Public Key Infrastructure Certificate and Certificate Revocation List Profile" provisions.

7.2 Certification Authority Revocation List and Certificate Revocation List Profile

7.2.1 Version Number

Certification Authority Revocation List and Certificate Revocation List shall comply with X.509 v2 provisions.

7.2.2 Extension Fields of the Certification Authority Revocation List and Certificate Revocation List

Every extension fields shall be defined in the "Government Public Key Infrastructure Certificate and Certificate Revocation List Profile".

7.3 Online Certificate Status Protocol profile

Certification Authority shall, if it provides the Online Certificate Status Protocol enquiry service, specify in the Certification Practice Statement regarding the service version number and the standard used on the extension fields; the response message shall add digital signature.

7.3.1 Version Number

Online Certificate Status Protocol's version number shall be in compliance with RFC 5019 and RFC 6960 provisions.

7.3.2 Extension Fields of the Online Certificate Status Protocol

The extension field for Online Certificate Status Protocol enquiry shall be in compliance with "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", RFC 5019 and RFC 6960 provisions published by ITU-T X.509 and CA/Browser Forum.

8 Audit Methods

Certification Authority with AL 2 level of assurance or above shall set up fair audit mechanism to ensure its operation comply with provisions of the Certification Practice Statement and the Certificate Policy.

NDC is entitled to audit Certification Authority to ensure that the Certification Authority comply with Certificate Policy provisions in carrying out various operation maintenance works. Certification Authority shall perform self-audit periodically to ensure its operation maintenance works are in compliance with the Certificate Policy's assurance level.

8.1 Audit Frequency or Assessment Particulars

Certification Authority shall be subject to periodic audit and comply with Schedule 8-1 "Certification Authority's Audit Frequency Provisions".

Schedule 8-1 Certification Authority's audit frequency

assurance level	audit frequency
test level	Certification Authority may decide at its own discretion. The Certificate Policy will not specify in this regard.
AL 1	Certification Authority may decide at its own discretion. The Certificate Policy will not specify in this regard.
AL 2	At least once every two years
AL 3	At least once a year
AL 4	At least once a year

Certification Authority shall conduct audit on its subordinate Certification Authority and the Registration Authority on a regular basis and as-needed basis to ensure its compliance with the operation of the Certification Practice Statement. Certification Authority shall, in the Certification Practice Statement, specify the minimum random check percentage on the Registration Authority.

8.2 Identity and Qualifications of the Audit Personnel

The auditors shall be independent of the audited Certification Authority, who can be served by the following entities:

(1) A just third-party;

(2) Another independent entity that is different from the audited Certification Authority In terms of organizational division.

The auditors shall provide just and independent assessment. Its qualifications shall be approved by the NDC, and it shall be familiar with provisions relating to the Certification Authority's certificate issuance and management. Certification Authority shall perform identity identification on the auditors before the audit.

8.3 Relationship Between the Audit Personnel and the Audited Party

In addition to the provision where the auditors shall be independent of the audited Certification Authority, its qualifications shall be pursuant to Section 8.2 “Identity and Qualifications of the Audit Personnel” provisions.

8.4 Scope of Audit

The scope of audit is prescribed as follows:

(1) Check if the Certification Authority comply with the operation of the Certification Practice Statement;

(2) Check if the Certification Authority’s Certification Practice Statement comply with regulations of the Certificate Policy.

The auditors shall carry out audit on the operation maintenance units such as the Registration Authority of the Certification Authority. If the Certification Authority entered into Cross-Certification Agreement with its subordinate Certification Authority, the scope of audit shall cover that subordinate Certification Authority to see whether it complies with the provisions of the Cross-Certification Agreement.

8.5 Ways to Cope with Audit Results

The auditors shall, if the Certification Authority’s setup and operation maintenance are found non-conforming with the Certificate Policy or provisions of the Cross-Certification Agreement, take the following actions:

(1) The auditors shall record non-conforming circumstances;

(2) The auditors shall notify the occurance of non-conforming circumstances to the Certification Authority’s competent authority. If the non-conforming circumstances is a severe deficiency, the auditors shall promptly notify NDC.

The Certification Authority having non-conforming circumstances shall perform correction based on the audit report, Certificate Policy or provisions of the Cross-Certification Agreement.

For the Certification Authority non-conforming with the audit standard requirements, NDC may require it to show improvement within a certain period of time or take other necessary measures.

8.6 Scope of Disclosure of Audit Results

The certificate information trusted by the relying party shall be publicly available unless such information may lead to system security risks or subject to Section 9.3 “Confidentiality of Business Information” provisions.

Certification Authority shall publish the latest audit results.

9 Other Business and Legal Particulars

9.1 Fees

Certification Authority may, based on its business needs, determine whether or not it shall charge fees on certificate related operation. The Certificate Policy will not specify in this regard.

9.1.1 Certificate Issuance and Renewal Fees

Certification Authority may, at its own discretion, determine the certificate issuance and certificate renewal fees. The Certificate Policy will not specify in this regard.

9.1.2 Certificate Enquiry Fee

Certification Authority may, at its own discretion, determine the certificate enquiry fee. The Certificate Policy will not specify in this regard.

9.1.3 Certificate Revocation and Status Enquiry Fees

Certification Authority may, at its own discretion, determine the certificate revocation and certificate status enquiry fees. The Certificate Policy will not specify in this regard.

9.1.4 Other Service Charges

Certification Authority may, at its own discretion, determine other service fees. The Certificate Policy will not specify in this regard.

9.1.5 Refund Request Procedures

Certification Authority may, at its own discretion, determine the refund application procedures. The Certificate Policy will not specify in this regard.

9.2 Financial Responsibility

Certification Authority may plan for its financial insurance responsibility based on its business concern. The Certificate Policy will not specify in this regard.

9.2.1 Scope of Insurance

Certification Authority may, at its own discretion, determine the scope of financial insurance for its certificate services. The Certificate Policy will not specify in this regard.

9.2.2 Other Assets

Certification Authority may, at its own discretion, determine the financial responsibility of other assets. The Certificate Policy will not specify in this regard.

9.2.3 Insurance or Warranty Responsibility to End Entity

Certification Authority may, at its own discretion, determine its insurance or warranty responsibility to the end entity. The Certificate Policy will not specify in this regard.

9.3 Confidentiality of Business Information

9.3.1 Scope of Sensitive Information

Certification Authority shall, in the Certification Practice Statement, specify the scope and type of sensitive information, which shall be handled pursuant to the relevant laws and regulations.

9.3.2 Scope of Non-Sensitive Information

Certification Authority shall, in the Certification Practice Statement, specify the scope and type of non-sensitive information.

9.3.3 Responsibility in the Protection of Sensitive Information

Certification Authority shall, in the Certification Practice Statement, specify the responsibility in the protection of sensitive information.

9.4 Privacy Nature of Personal Information

9.4.1 Privacy Protection Plan

Certification Authority shall, in the Certification Practice Statement, specify personal data protection and privacy statement.

9.4.2 Type of Private Information

Certification Authority shall, in the Certification Practice Statement or website, specify the type of private information.

9.4.3 Non-Private Information

Certification Authority shall, in the Certification Practice Statement, specify the type of non-private information.

9.4.4 Responsibility in the Protection of Private Information

Certification Authority shall, in the Certification Practice Statement, specify the responsibility in the protection of private information.

9.4.5 Announcement and Consent in the Use of Private Information

Certification Authority shall, in the Certification Practice Statement, specify the regulation regarding the use of private information.

9.4.6 Information Released Due to Judicial or Administrative Procedures

Certification Authority shall, in the Certification Practice Statement, specify the regulation relating to the provisions of private information to judicial personnel.

9.4.7 The Release of Other Information

Certification Authority shall, in the Certification Practice Statement, specify the regulation relating to the provisions of other information, which shall be handled pursuant to the relevant laws and regulations.

9.5 Intellectual Property Rights

The intellectual property rights of the Certificate Policy is owned by NDC. The related information can be downloaded from the Root Certification Authority's repository or be reproduced or distributed pursuant to the related provisions of the copyright law, provided that, the copy shall be complete and specify the copyright ownership. In addition, the reproduction or distribution of the Certificate Policy shall not involve fees charged on others and shall not refuse anybody's request in obtaining the Certificate Policy. NDC will not be bear any legal liability for any problem arising from the inproper use or distribution of the Certificate Policy.

9.6 Duties and Obligations

9.6.1 Certification Authority's Duties and Obligations

Certification Authority's duties and obligations shall include at least the following particulars:

(1) To comply with the Certificate Policy's provisions;

(2) To perform the identification and authentication on certificate application;

(3) To issue and publish certificates;

(4) To revoke certificates;

(5) To issuce and publish the Certification Authority Revocation List or the Certificate Revocation List;

(6) To issue and provide response message for the Online Certificate Status Protocol enquiry service;

(7) To perform identification and authentication on CA personnel;

(8) To securely generate CA private keys;

(9) To protect CA private keys;

(10) To publish the Certification Practice Statement and specify the subscriber's and relying party's responsibilities.

9.6.2 Registration Authority's Duties and Obligations

Registration Authority's duties and obligations shall include at least the following particulars:

(1) To provide certificate application service;

(2) To perform identification and authentication on certificate applications;

(3) To inform the subscriber's and relying party's regarding the obligations and responsibility of the Certification Authority and Registration Authority;

(4) To perform identification and authentication on certificate registration review personnel;

(5) To manage the Registration Authority's private keys;

(6) The Registration Authority shall not use the RA private key in the operation outside the scope registered in the certificate without its superior Certification Authority's consent.

9.6.3 Subscriber's Obligations

The subscriber's obligations shall include at least the following particulars:

(1) To provide accurate and complete information;

(2) To comply with relevant provisions of the Certificate Policy and the Certification Practice Statement;

(3) To safeguard and use the private key appropriately;

(4) To promptly notify the Certification Authority and suspend the certificate when the private key is used without its consent, compromised or lost;

(5) To securely generate its private key and avoid been compromised.

9.6.4 Relying Party's Obligations

The relying party's obligations shall include at least the following particulars:

(1) To use the certificate pursuant to the certificate and the certificate's assurance level and applicability;

(2) To accurately check the certificate's digital signature, validity and key usage pursuant to the provisions of the Certificate Policy or Certification Practice Statement;

(3) To ensure a secure environment for the use of the certificate and bear the responsibility not attributable to the Certification Authority;

(4) Relying party shall, when the Certification Authority cannot operate normally, seek other means to complete its legal acts with others at its earliest convenience and shall not use Certification Authority's failure to operate normally as the reason in dispute with others.

9.6.5 Other Participant's Obligations

Certification Authority may, at its own discretion, determine other participants' obligations. The Certificate Policy will not specify in this regard.

9.7 Disclaimer

Certification Authority shall, in the Certification Practice Statement, specify disclaimer and its constraints, provided that, the consequences attributable to its own negligence shall not be included in the disclaimer.

9.8 Responsibility and Constraints

Certification Authority shall, in the Certification Practice Statement, specify the responsibility and constraints. Certification Authority shall, if there is any issuance SSL

certificate, comply with the requirements of the official version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" Published by CA/Browser Forum.

9.9 Indemnity

Certification Authority shall, in the Certification Practice Statement, specify the indemnity responsibility to the subscribers and relying party, which shall be in compliance with the Electronic Signatures Act and the related laws and regulations.

9.10 Expiration Date and Termination

Certification Authority shall, in the Certification Practice Statement, specify the expiration date and termination.

9.10.1 Expiration Date

This Certificate Policy and its Appendix are effective upon announcement on the GPKI website and repository.

9.10.2 Termination

The termination of Certificate Policy is subject to the Government Electronic Certification Steering Committee's authorization.

9.10.3 Termination and Duration Effects

The Certificate Policy shall remain effective after its termination until the last certificate become invalid.

9.11 Individual Notification and Communication with the Participants

Individual notification and communication with the participants shall be carried out by appropriate means.

9.12 Revision

(1) The Certificate Policy shall be reviewed at least once a year. Certification Authority shall review the Certification Practice Statement at least once a year.

(2) The Certification Authority providing SSL certificate issuance and management services shall perform annual review and ensure the Certification Practice Statement complies with the requirements of the official version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" Published by CA/Browser Forum; ; if there is any inconsistence between the Certification Practice Statement and the aforesaid forum specification, the Certification Practice Statement will be revised pursuant to the provisions of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published by the CA/Browser Forum and authorized by the competent authority – Ministry of Economic Affairs – duly identified in the Electronic

Signatures Act before implementation.

9.12.1 Revision Procedures

The Certificate Policy amendment is subject to the review by Government Electronic Certification Steering Committee before promulgation.

9.12.2 Notification Mechanism and Deadline

Certification Authority shall announce any modifications that may cause major impact on the subscribers in the repository. Certification Authority shall, in the Certification Practice Statement, specify the notification mechanism and announcement period for the modifications.

Certification Practice Statement revision shall be announced within 10 calendar days after obtained the approval from the competent authority duly identified in the Electronic Signatures Act.

9.12.3 Causes for the Revision of Certificate Policy Object Identifier

Certificate Policy Object Identifier shall be modified by the following causes:

(1) When the assurance level defined in the Certificate Policy is changed;

(2) When it is assessed that changes shall be made in response to international environmental changes or regulatory changes.

9.13 Dispute Processing Procedures

Certification Authority shall, in the Certification Practice Statement, specify the dispute processing procedures.

9.14 Governing Law

GPKI shall be subject to the laws of the Republic of China in performing its business.

9.15 Applicable Laws

GPKI shall perform its business pursuant to the relevant laws and regulations. Certification Authority shall, in the Certification Practice Statement, specify the applicable laws.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Certification Authority may, at its own discretion, determine the entire agreement with the contracting party of its Certification Practice Statement. The Certificate Policy will not specify in this regard.

9.16.2 Assignment

Certification Authority shall, in the Certification Practice Statement, specify the provisions regarding the assignment of primary member’s right or responsibility.

9.16.3 Severability

The Certificate Policy shall remain valid even when any of its sections becomes not

applicable and subject to amendment.

The Certificate Policy also complies with the requirements of the official version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" Published by CA/Browser Forum, , provided that, if its related provisions are in contrary with the relevant laws or regulations abinded by the Certificate Policy, the Certificate Policy may make slight adjustment on the related practice to fulfill the requirements of the laws or regulations and notify CA/Browser Forum of such modification / adjustment. The adjusted contents of the original policy will, in the occurance of following circumstances, be deleted and revised upon the Government Electronic Certification Steering Committee's authorization. The aforesaid operation shall be completed within 90 days.

(1) When the laws or regulations in contrary with the relevant provisions of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" Published by CA/Browser Forum were amended or deleted;

(2) When the CA/Browser Forum revised the related contents of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" to accommodate with the laws and regulation of the Republic of China.

9.16.4 Contract Performance

Whereas the subscriber or the relying party violates the relevant provisions of the Certificate Policy, causing the Root Certification Authority to suffer damages, if the responsibility is attributable to the subscriber or the relying party's intentional act or negligent, the Root Certification Authority may, in addition to claiming for compensation, ask either of the attributable parties to pay for the attorney's fees associated with the dispute or litigation process.

The Root Certification Authority's hold back on claiming its rights from the one who violated the Certificate Policy does not mean that the Root Certification Authority waived the right to claim its rights in any subsequent or future violation against the Certificate Policy.

9.16.5 Force Majeure

The Certification Authority shall not be held liable for any damages caused by force majeure and other factors not attributable to the Certification Authority.

Certification Authority may, in the Certification Practice Statement, specify the exemption provisions, provided that, mistakes arising from its own negligence shall not be listed in the exemption provisions.

9.17 Other Provisions

Certification Authority may, at its own discretion, define other provisions based on its needs. The Certificate Policy will not specify in this regard.

Appendix 1: Term Definitions

- **A**
  - **Activation Data:** Private data required besides keys to access cryptographic module (such as data used to activate private key for signatures or encryption).
  - **American Institute of Certified Public Accountants, AICPA:** The unit jointly enacted "The Trust Services Principles and Criteria for Secure, Availability, Processing Integrity, Confidentiality and Privacy" standards with Chartered Professional Accountants Canada, and the administrator of the marks of the WebTrust for CA, SSL Baseline Requirement & Network Secure.
  - **Applicant:** Subscriber who applies for certificate from a Certification Authority but have not yet completed the certification procedures.
  - **Archive:** A physically separate (from the storage site of primary information) storage site for long-term information, which can be used to support audit, usage and integrity services.
  - **Assurance:** A reliable basis to determine that an entity conforms to certain security requirements.
  - **Assurance Level:** A level possessing a relative assurance level.
  - **Audit:** Assessment on whether system controls are adequate to ensure conformance with the existing policy and operation procedure, while being independent in reviewing and investigating the recommended necessary improvements on current controls, policies and procedures.
  - **Audit Log:** System activity logs sorted by time of occurrence, which can be used to reconstruct or investigate the time sequence or changes occurred in a certain event.
  - **Authenticate:** The process of verifying legitimacy of the identity of a certain entity.
  - **Authentication:**
    - The procedures used to establish the reliability of the identity of the administrator or information system.
    - The means to establish security measures used for information transmit, messages and sources, or the authority to to verify whether individuals have received certain types of information.
- **C**
  - **Certificate:**
    - Refers to the verification information carrying a digital signature used to verify the identity and qualifications of the signatory in electronic form.
    - Digital presentation of information, which includes the the contents:

- ✓ Issuing Certification Authority;
- ✓ Subscriber's name or identity;
- ✓ Subscriber's public key;
- ✓ Certificate validity period;
- ✓ Certification Authority's digital signature.

- **Certificate Policy (CP):** An administrative policy with dedicated profile set for the electronic transactions performed through certificate administration. The Certificate Policy covers a variety of issues including the formation, generation, transmission, auditing, post-compromise recovery and administration of digital certificates. Certificate Policy and its related techniques can provide secure services required for specific application.
- **Certificate Revocation List (CRL):**
  - Certificate revocation list is digitally signed by Certification Authority available to be used by the relying party.
  - A list maintained by Certification Authority, which listed the certificates issued by the Certification Authority and revoked before their expiry dates.
- **Certification Authority (CA):**
  - The agency or natural person that issues certificates.
  - The competent body trusted by the subscribers. Its functions are to issue and administer X.509 format public key certificates, Certification Authority Revocation List and Certificate Revocation List.
- **Certification Authority Authorization (CAA):** Pursuant to RFC 6844 provisions, the Certification Authority Authorization DNS Resource Record permit the domain owner in the domain name system to designate a Certification Authority (one or more) to obtain authorization in issuing certificate for the domain. The Certification Authority Authorization DNS Resource Record permit publicly trusted Certification Authority to implement additional control to reduce unexpected certificate mis-issuance risk.
- **Certification Authority Revocation List (CARL):** A signed and time stamped list. The list contains the serial numbers of revoked CA public key certificates (including cross-certificates of the subordinate Certification Authority).
- **Certificate Modification:** Refers to the provision of a new certificate in replacement of the original certificate to the same subject, provided that, the expiration date of the new certificate shall be the same as that of the old certificate. The original certificate shall be revoked after the modification.

- **Certification Practice Statement (CPS):**
  - External notification by the certificate authority used to describe the practice statement of the certificate authority governing certificate issuance and processing of other certification work.
  - Announcement of a statement that certain procedures of the certificate authority for certificate work (including issuance, suspension, revocation, renewal and access) comply with certain requirements (listed in the certificate policy or other service contracts).
- **Chartered Professional Accountants Canada (CPA):** The unit jointly enacted "The Trust Services Principles and Criteria for Secure, Availability, Processing Integrity, Confidentiality and Privacy" standards with American Institute of Certified Public Accountants, and the administrator of the marks of the WebTrust for CA, SSL Baseline Requirement & Network Secure. Chartered Professional Accountants Canada, formerly named as "Canadian Institute of Chartered Accountants (CICA)".
- **Compromise:** Information disclosed to unauthorized persons or unauthorized intentional or unintentional disclosure, modification, destruction or loss of objects which constitutes a violation of information security policy.
- **Cross-Certificate:** A type of certificate that establishes a trust relationship between two root certification authorities and is regarded as a CA certificate, not a subscriber certificate.
- **Cross-Certification:** The act or procedures of a Certification Authority under a public key infrastructure issuing a public key certificate to another Certification Authority under a public key infrastructure.
- **Cross Certification Agreement (CCA):** The agreement containing the terms and individual liability and obligations that must be followed when the government root certification authority and subordinate certification authorities apply to join the government authority public key infrastructure.
- **Cryptographic Module:** A set of hardware, software, firmware or combination of the above used to run cryptologic or programs (including cryptoalgorithms) and included within the cryptographic boundaries of the module.

◆ **D**

- **Digital Signature:** An electronic signature generated by the use of mathematic algorithm or other means to create a certain length of digital data encrypted by the signatory's private key and capable of being verified by the public key.
- **Duration:** A certificate field made up on two subfields, "start time of the validity

period" and "end time of the validity period".

◆ **E**

- **End Entity (EE):** including the following two types of entities in the GPKI：
  - The private key owner responsible for keeping and applying certificates;
  - A third party receiving certificate issued by trusted GPKI Certification Authority (not the private key owner and not the Certification Authority), that is, the End Entity is the subscribers and relying parties (including persons, organizations, accounts, devices and sites).

◆ **F**

- **Federal Information Processing Standard (FIPS):** The information process standard used by all government agencies and government contractors (excluding military agencies) formulated by the U.S. federal government, where the standard security clearance requirements of the cryptographic module are FIPS 140; FIPS 140-2 classifies cryptographic modules into 11 types of security requirements, and each security requirement is subdivided into 4 security levels.

◆ **G**

- **Government Root Certification Authority:** A GPKI Root Certificate Authority, which is the highest level certificate authority in public key infrastructure hierarchy and the trust anchor of public keys.

◆ **I**

- **Identity Assurance Level:** One of the levels used in identity authentication with a relative degree of guarantee.
- **Internet Engineering Task Force (IETF):** responsible for the development and promotion internet standard. Its mission is to impact human design, use and management of the internet via the generation of high-quality technical document to make the internet operates more smoothly. (official website: https: //www.ietf.org).
- **Issuing CA: Issuing CA**: in terms of the certificate, the Certification Authority that issued the certificate is certificate's Issuing CA.

◆ **K**

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

agreement.

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

◆ **M**

- **Mutual Authentication:** When two parties authenticate one another during communication activities.

◆ **O**

- **Object Identifier (OID)**
  - Refers to a unique alphanumeric / numeric identifier registered under the International Standard Organization registration standard and which could be used to identify the uniquely corresponding certificate policy.
  - When a special form of code, object or object type is registered with the International Organization for Standardization, the unique code may be used as an identifier. For example, this code can be used in the public key infrastructure to indicate what certificate policy and cryptographic algorithms are used.
- **Online Certificate Status Protocol (OCSP):** An online certificate checking protocol allowing the relying party's application software to determine the status (such as revocation status, its validity, etc.) of a particular certificate.
- **Organization Validation (OV):** In the process of issuing an SSL certificate, in addition to identifying and authenticating the subscriber's domain name control rights, the subscriber's organization or individual identity is identified and authenticated according to the certificate's assurance level. Therefore, it is possible to link to a website that installs organization-proven SSL certificates to provide TLS-encrypted channels, to know who owns the site, and to ensure the integrity of the transmitted data.

◆ **P**

- **Private Key:** this key shall be kept confidential under the following two circumstances
  - The key in the signature key pair used to generate digital signatures;
  - The key in the encryption key pair used to decrypt secret information.
- **Public Key**: the key shall be made publicly available under the following two

circumstances (usually in a digital certificate form).

- The key in the signature key pair used to verify the validity of the digital signature.
- The key in the encryption key pair used for encrypting confidential information.

- **Public Key Infrastructure (PKI)**：Develop and manage asymmetric cryptography and public key certificates on a vast scale covering laws, policies, regulations, personnel, equipment, facilities, technologies, processes, audits, and services.

◆ **R**

- **Registration Authority (RA)**
  - Responsible for checking the identity and other attributes of the certificate applicant but does not issue or administer certificates. The nature and scope of obligations borne by the registration authority are set down in the applicable certificate policy or agreement.
  - An entity responsible for the identification and authentication of the certificate subject identity which does not issue certificates.
- **Re-key a Certificate:** Re-key a Certificate refers to the issuance of a new certificate with the same characteristics and level of assurance as the old certificate, except that the new certificate has a brand new and distinct public key (corresponding to a new and different private key) and a different serial number, even a different expiration date.
- **Relying Party**
  - Recipient of a certificate who acts in reliance of that certificate or a digital signature to verify the public key listed in the certificate, or the counterparty to identity (or its attributes) of the subject named in a trusted certificate and public key listed in the certificate.
  - The individual or agency which receives information which includes a certificate and digital signature (the public key listed on the certificate may be used to verify this digital signature) and may rely on this information.
- **Renew a Certificate:** The procedure for issuing a new certificate with new serial number to renew the old certificate bearing the same subject name, key and relevant information in order to extend the validity.
- **Repository**
  - A trustworthy system used to store and retrieve certificates or other information relevant to certifications.
  - The repository containing the certificate policy and certificate-related

information.

- **Revoke a Certificate:** Termination of a certificate prior to its expiry date.
- **Root Certification Authority (Root CA):** the highest-level Certification Authority in public key infrastructure. In addition to issuing subordinate CA certificates and self-signed certificates, its self-signed certificate shall be distributed by application software vendors.

◆ **S**

- **Self-Issued Certificate:** The self-issued certificate is issued by the Root Certification Authority when the replacement of key or Certificate Policy is needed. The two generations of Root Certification Authorities use their private keys to issue each other to establish the trust path between the old and new keys or between one Certificate Policy and another Certificate Policy.
- **Self-Signed Certificate:** A self-signed certificate is a type of certificate where the issuer name is the same as that of the subject. That is, using the same pair of private key to issue certificates for the public key and other information in the paired relationship. A self-signed certificate within the public key infrastructure can be used as the trust anchor of the certificate path. Its issuance subject is the Root Certification Authority itself, which contains the public key of the Root Certification Authority and bearing the same issuer name as that of the subject, to allow the relying party to verify the digital signature on the self-issued certificate, subordinate Certification Authority certificate, cross-certificate and Certification Authority Revocation List issued by the Root Certification Authority.
- **Subject Certification Authority:** For a CA certificate, the certificate authority referred to in the certificate subject of a certificate is the subject CA for that certificate.
- **Subordinate Certification Authority:** In the public key infrastructure hierarchy, certificates that are issued by another certificate authority and the activities of the certificate authority are restricted to this other certificate authority.
- **Subscriber**
  - Refers to a subject named or identified in the certificate that holds the private key that corresponds with the public key listed in the certificate.
  - An entity having the following attributes including (but not restricted to) individuals, organizations and network devices:
    - ✓ Entity listed on an issued certificate;
    - ✓ A private key that corresponds to the public key listed in the

certification;

- ✓ Other parties that do not issue certificates.

◆ **T**

- **Trust Anchor:** The starting certificate of the trust path, which is trusted by the relying party and is obtained via a secure and reliable transmission method.
- **Trustworthy System:** Computer hardware, software and programs which possess the following attributes:
  - Functions that protect again intrusion and misuse;
  - Provides reasonably accessible, reliable and accurate operations;
  - Appropriate implementation of preset function;
  - Security procedures uniformly accepted by the general public.

◆ **Z**

- **Zeroize:** Method to delete electronically stored information. Storage of changed information to prevent information recovery.

Appendix 2: BRs-Section 1.2.1 Revisions

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

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

1.4.4	193	825-day Certificate Lifetimes	17-Mar-2017	1-Mar-2018	Compliant
1.4.5	189	Amend Section 6.1.7 of Baseline Requirements	14-Apr-2017	14-May-2017	Compliant
1.4.6	195	CAA Fixup	17-Apr-2017	18-May-2017	Compliant
1.4.7	196	Define “Audit Period”	17-Apr-2017	18-May-2017	-
1.4.8	199	Require commonName in Root and Intermediate Certificates 9	9-May-2017	8-June-2017	Compliant
1.4.9	204	Forbid DTPs from doing Domain/IP Ownership	11-July-2017	11-Aug-2017	Compliant
1.5.0	212	Canonicalise formal name of the Baseline Requirements	1-Sept-2017	1-Oct-2017	Compliant
1.5.1	197	Effective Date of Ballot 193 Provisions	1-May-2017	2-June-2017	Compliant
1.5.2	190	Add Validation Methods with Minor Corrections	19-Sept-2017	19-Oct-2017	Compliant
1.5.3	214	CAA Discovery CNAME Errata	27-Sept-2017	27-Oct-2017	Compliant
1.5.4	215	Fix Ballot 190 Errata	4-Oct-2017	5-Nov-2017	Compliant
1.5.5	217	Sunset RFC 2527	21-Dec-2017	20-Jan-2018	Compliant
1.5.6	218	Remove validation methods #1 and #5	5-Feb-2018	9-Mar-2018	Compliant
1.5.7	220	Minor Cleanups (Spring 2018)	30-Mar-2018	29-Apr-2018	Compliant
1.5.8	219	Clarify handling of CAA Record Sets with no "issue"/"issuewild" property tag	10-Apr-2018	10-May-2018	Compliant
1.5.9	223	Update BR Section 8.4 for CA audit criteria	15-May-2018	14-June-2018	Compliant
1.6.0	224	WhoIs and RDAP	22-May-2018	22-June-2018	Compliant
1.6.1	SC6	Revocation Timeline Extension	14-Sep-2018	14-Oct-2018	Compliant
1.6.2	SC12	Sunset of Underscores in dNSNames	9-Nov-2018	10-Dec-2018	Compliant
1.6.3	SC13	CAA Contact Property and Associated E-mail Validation Methods	25-Dec-2018	1-Feb-2019	Compliant
1.6.4	SC14	Updated Phone Validation Methods	31-Jan-20	31-Jan-20	Compliant
	SC15	Remove Validation Method Number 9	5-Feb-2019		
	SC7	Update IP Address Validation Methods	8-Feb-2019		

1.6.5	SC16	Other Subject Attributes	15-Mar-2019	16-April-2019	Compliant

* Effective Date and Additionally Relevant Compliance Date(s)