Certificate Practice Statement of the Trusted Network Service Center of the China Internet Network Information Center (CNNIC)

Version No.: 3.06

Period of validity: from April 26th, 2015 to April 26th, 2016

China Internet Network Information Center (CNNIC)

April 26th, 2015

CPS Version Control of the Trusted Network Service Center of CNNIC

Version No.	Revise Description	Finish Date
V1.00		2007-5-15
V2.00	Extended the expiration of CPS to one year with anuual audit	2008-4-8
V2.01	Offer CRL download through http agreement	2008-11-5
V2.02	1. Key pair of Domain Name certificate requires 2048 bits 2. Revised the compensation ammout 3. Revised postcode of contact information 4. Extended the expiration of CPS to one year with anuual audit	2009-3-19
V2.03	1. Revised Organization attribution in Certificate Subject 2. Revised CN attribution in Certificate Subject of Multi-domain Name certificates. 3. Adjusted application meterias 4. Adjusted certificate deccription in certificate profile, and keep the consistence with certificate issued.	2009-4-14
V2.04	1. Adjust the method of the reference number and authorization code's release 2. Publish CP in repository 3. Adjust the explaination of situation of Certificates publishment	2009-6-18
V2.05	1. Revise the description on cross signing and insert the explanation of the relationship between CNNIC intermediate root and Entrust root certificates.	2009-11-09
V 2.06	Increase the description of CRL issued by CNNIC root, and revise the relative words	2010-2-2
V 2.07	Revise expiration	2010-4-7
V3.0	1. Increase the relevant content of domain quick certificate. 2. Modify the work method of security management committee.	2011-4-7

	3. Cancellation of external ldap service.	
V3.01	1. "Advanced Certificate" is changed into "Standard Server Certificate"; the name of "Website Guard" is deleted, and paper Website Guard Ratification Instruction will not be provided anymore; and standard certificate auditing contents are modified; 2. Relevant procedures of domain quick certificate are modified; CPS valid period is extended one year;	2012-6-31
V3.02	1. Materials required for standard server certificate application were modified; 2. Information on personnel background investigation related to CA was revised; 3. Information related to electromagnetic protection was added	2012-8-9
V3.03	1. The application materials submitted by local service provider to CNNIC were changed into electronic scanned copy from paper-based original copy; 2. Verification and confirmation of standard server certificate requires only phone confirmation with the operator; 3. CA service system downtime and recovery time in the case of disaster was added to the disaster recovery plan.	2013-6-24
V3.04	1. Stop service for multi-domain certificate changes. 2. CNNIC commit to comply SSL Baseline Requirement of CABForum. 3. Establishing 24*7 emergency processing of CNNIC CA.	2014-4-22
V3.05	1. Adjust the method of the reference number and authorization code's release, the full 16 number will be released to applicant.	2015-1-20
V3.06	1. Add chapter 5, Operation specification of Subordinate CA authorization 2. In Chapter 8, add Suboridinate CA certificate structure。	2015-4-26

Contents

1 Introduction

1.1 Overview

The Trusted Network Service Center of the China Internet Network Information Center (CNNIC) (hereinafter referred to as CNNIC Trusted Network Service Center) provides domain names with domain name certificate security service, and has thereby, in accordance with the compilation rules of the IETF on Certificate Practice Statement (CPS), compiled the CPS of CNNIC Trusted Network Service Center as the codes for the certificate-related services and system operations of CNNIC Trusted Network Service Center.

1.2 Roles and Responsibilities

1.2.1 Security Management Committee

The Security Management Committee of CNNIC Trusted Network Service Center is responsible for the formulation of security strategies, creteria and decision making, and is the decision-making department in charge of security management of CNNIC Trusted Network Service Center. The responsibilities of the Security Management Committee include: collecting and coordinating problems and suggestions in terms of security management and reaching consistent opinions; developing and maintaining Certificate Policies (CP) of CNNIC Trusted Network Service Center; examining this CPS so as to ensure the CPS is consistent with Certificate Policy documents.

The Security Management Committee shall hold one meeting every year or preceded a document countersign to check and approval the relevant systems and regulations of CNNIC Trusted Network Service Center, and then annouce about operational status of CNNIC Trusted Network Service Center.Besides, if there are other important changes, the Security Management Committee should be based on the actual documents in a

timely manner meeting or by the way of countersigned on important issues for discussion and approval. The members of the Committee are composed of representatives of the CNNIC leaders, human resources, finance, legal affairs and security management etc.

1.2.2 Chief Security Administrator

The Chief Security Administrator will be responsible for each daily security affair of CNNIC Trusted Network Service Center and be authorized by the Security Management Committee of CNNIC Trusted Network Service Center. The Chief Security Administrator may alter the security policy of CNNIC Trusted Network Service Center, carry out regular check and evaluation of security management of CNNIC Trusted Network Service Center, and maintain the security management of CNNIC Trusted Network Service Center on an advanced level, with high degree of security and reliability. Also, it will follow the latest development in terms of security management at all times to ensure that the security system can be up to an advanced level. To safeguard the security and reliable operation of CNNIC Trusted Network Service Center, the Chief Security Administrator of CNNIC Trusted Network Service Center shall focus its attention on the following three key fields: developing security policy and assisting program development and implementation; maintaining security policy and programs to keep their completeness; auditing security policy and the consistency of its actual implementation.

The Chief Security Administrator of CNNIC Trusted Network Service Center has the following responsibilities:

◆ After being authorized, establishing and altering the security policy and creterias of CNNIC Trusted Network Service Center;

◆ Managing cross certificates, releasing the cross certificates agreement of CNNIC Trusted Network Service Center, updating and cancelling cross certificates;

◆ Handling auditing reports.

1.3 Applicability

1.3.1 CNNIC Trusted Network Service Center

According to this CPS, CNNIC Trusted Network Service Center shall perform the function as a Certificate Authentication agency and assume its obligations. CNNIC Trusted Network Service Center is the only Certificate Authentication agency authorized by this CPS to issue certificates (see Section 2.1.1).

1.3.1.1 Statement made by CNNIC Trusted Network Service Center

CNNIC Trusted Network Service Center states clearly to the relying parties observing Section 2.1.5 of this CPS and other related terms that CNNIC Trusted Network Service Center issues certificates to the certificate subscribers in accordance with this CPS.

1.3.1.2 Effectiveness

The certificates issued by CNNIC Trusted Network Service Center shall immediately take effect when they are issued and accepted by the certificate subscribers.

1.3.1.3 Rights authorized by CNNIC Trusted Network Service Center to Local Registration Authority (LRA)

CNNIC Trusted Network Service Center may authorize the responsibilities of part or all of the work to perform this CPS and certificate subscribers' agreement to Local Registration Authority (LRA). Whether or not the related responsibilities are fulfilled by Local Registration Authority (LRA), CNNIC Trusted Network Service Center will still be responsible for performing this CPS and certificate subscribers' agreement.

Local Registration Authority (LRA) in this practice statement refers to the CNNIC SSL Certificates registration service agencies certified by the CNNIC.

1.3.2 Final entities

According to this Certificate Practice Statement, there are two types of final entities, including certificate subscribers and relying parties. A certificate subscriber may be a "certificate holding individual" or a "certificate holding organization". Relying parties trust any kind or type of certificates (including but not limited to domain name certificates) issued by CNNIC Trusted Network Service Center. It is hereby clarified that what the relying parties trust are not certificate registration agencies such as the Registration Authority (RA) of CNNIC Trusted Network Service Center or Local Registration Authorities, but CNNIC Trusted Network Service Center. CNNIC Trusted Network Service Center issues digital certificates via the Registration Authority, but the Registration Authority doesn't have duty or responsibility for the relying parties and does not have to be responsible for issuing digital certificates to the relying parties (see Section 2.1.2).

1.3.2.1 Pledge and statement of certificate subscribers

An applicant shall sign or determine to accept an agreement (according to the terms stipulated in this CPS), on which there is one term, on the basis of which the applicant agrees that the applicant's acceptance of a certificate issued according to this CPS shows that the applicant pledges (promises) to CNNIC Trusted Network Service Center and states to other related parties (especially the relying parties) that within the usage period of the certificate the following facts are true and their truthfulness will be maintained:

◆ Besides domain name certificate subscribers and the parties being authorized, no other people have got and used the private key.

◆ Each digital signature produced in the use of the certificate subscribers' private key related to the public key included in the certificate subscribers' domain name certificate is truly the certificate subscribers' digital signature.

◆ All the information included in the certificate and the statement made by the

certificate subscribers is true.

◆ The certificate will only be used for lawful purposes approved in this CPS.

◆ All the materials provided in the course of certificate application shall not violate any third party's trademark, service mark, company name or any intellectual property right.

1.3.3 Classification of certificate subscribers

The certificate subscribers of CNNIC Trusted Network Service Center are domain name subscribers, who may be legal persons or natural persons. Yet CNNIC Trusted Network Service Center does not distinguish them.

1.3.4 Classification of certificates

CNNIC Trusted Network Service Center provides domain name certificate service (also referred to as "Website Guard" service) according to this CPS. The brand of the domain name certificates issued at present is "SSL certificate" and "DQ certificate", SSL certificate has different types:

◆ Single domain certificate: CN is a fixed domain name

◆ Wildcard domain certificate: CN is a domain name whose format is "*.xxx.xxx"

◆ Multi-domain certificate: CN is composed by many domains, like CN=a.xxx.xxx, CN=b.xxx.xxx, CN=c.xxx.xxx. And SAN extension includes these many domain names.

The SSL certificates issued by CNNIC Trusted Network Service Center are only limited to domain name certificates, ensure that the encrypted transmission of information, and also further reflect the entity information in the certificate, but it cannot be used for other purposes.

Different types of DQ certificates:

◆ Single domain certificate: CN is a fixed domain name

◆ Multi-domain certificate: CN is composed by many domains, like CN=a.xxx.xxx, CN=b.xxx.xxx, CN=c.xxx.xxx. And SAN extension includes these many domain names.

The DQ certificates issued by CNNIC Trusted Network Service Center are only limited to domain name certificates, ensure that the encrypted transmission of information transmission between site and client, but it cannot be used for other purposes.

1.3.5 Certificates' usage period

The usage period of the certificates issued to new applicants according to this certificate practice is one year.

The usage period of the certificates issued according to the certificate renewal procedure of this certificate practice may prolonged the above-mentioned usage period. Inside digital certificates, their usage period will be indicated.

1.3.6 Application for certificates with CNNIC Trusted Network Service Center

For all the first applications and applications after a certificate is revoked or expires, the applicants shall submit application according to the procedure stipulated in this CPS.

1.4 Contact information

Mailing address: CNNIC, P.O. Box 349-6, Beijing

Postal code: 100190

Tel.: 86-10-58813000

Fax: 86-10-58812666

Email address: service@cnnic.cn

Website: http://www.cnnic.cn

Chinese domain name: http://中国互联网络信息中心.CN

General website: 中国互联网络信息中心:CNNIC

1.5 Procedure for complaint handling

The working personnel of CNNIC Trusted Network Service Center will handle all the written and oral complaints as soon as possible and give detailed reply within five (5) working days. If no detailed reply can be given within five (5) working days, a brief reply will be made to the complainant. Within a feasible scope, the personnel of CNNIC Trusted Network Service Center will contact the complainant as soon as possible via telephone, email or mail and give a reply.

2 General Provisions

2.1 Obligations

The obligations of CNNIC Trusted Network Service Center to certificate subscribers are stipulated by this CPS and the certificate subscribers' agreement reached with the certificate subscribers. For the certificate relying parties who are non-certificate subscribers, CNNIC Trusted Network Service Center only promises to adopt reasonable technology to avoid several types of losses and damages incurred to the certificate relying parties when the certificate is issued or revoked according to this CPS, and sets limitations on liabilities.

2.1.1 Obligations of the Certification Authority (CA) of CNNIC Trusted Network Service Center

According to precedents, CNNIC Trusted Network Service Center is a recognized certificate authority center, responsible for using a stable system to issue and revoke certificates and using the open repository to release information such as the Certificate Revocation List. According to this CPS, the Certification Authority of CNNIC Trusted

Network Service Center has the following obligations:

a) Receiving the request of the Registration Authority and issuing certificates in time

b) Revoking certificates and releasing the Certificate Revocation List (CRL) (refer to Section 4.5)

c) CNNIC will check the requirement of SSL Baseline Requirement regularly , commit to upgrade CA system and adjust CA business practice to meet the latest version of SSL Baseline Requirment.

d)

2.1.2 Obligations of the Registration Authority (RA) of CNNIC Trusted Network Service Center

The Registration Authority system is responsible for certificate applicants' applications and the examination and approval of these applications as well as certificate management, and passing on certificate application information to the Certification Authority. The Registration Authority has the following obligations:

a) According to the provisions of Chapter 3 and Chapter 4 in this CPS, verifying the accuracy and truthfulness of the information submitted by the applicants, making the certificate applications that pass verification take effect, and passing them safely on to the Certification Authority (CA). Certificate applications include various types of application such as certificate registration, reissue, renewal, revocation and multi-domain name change.

b) Notifying applicants of the certificate applications that have been approved or rejected (refer to Sections 4.1, 4.2, 4.3 and 4.4)

c) Notifying certificate subscribers of the certificates that have been revoked (refer to Section of 4.5.1, 4.5.2 and 4.5.3)

CNNIC Trusted Network Service Center has only one Registration Authority, which is set at the CNNIC.

CNNIC Trusted Network Service Center determines the identity of LRA and

authorizes LRA to collect information for registration of certificate applicants. LRA is obliged to be responsible for collecting related information and preliminarily verifying the correctness of such information when certificate applicants carry out certificate registration, reissue, renewal, revocation and multi-domain name modification.

2.1.3 The repository's obligations

The repository of CNNIC Trusted Network Service Center shall publicize the Certificate Revocation List (CRL) and other contents in time according to the policy it has developed.

2.1.4 Certificate subscribers' obligations

Certificate subscribers are responsible for:

a) Properly completing the application procedure and signing or determining to accept the certificate subscribers' agreement; performing the obligations that they shall assume according to the agreement and ensuring that the statement made in the application for certificates is correct.

b) Correctly comply with the procedure on completing a certificate described in this CPS.

c) Promising to use reasonable preventive measures to protect the confidentiality of the private key of their certificates (that is, to keep it confidential) and its completeness to prevent loss, disclosure or unauthorized use.

d) Immediately reporting its loss or disclosure to CNNIC Trusted Network Service Center upon discovering that the private key of their certificates is lost or disclosed.

e) Notifying in time any change of the information about the certificates of the certificate subscribers to CNNIC Trusted Network Service Center.

f) Immediately notifying CNNIC Trusted Network Service Center when one of circumstances stipulated in Section 4.5.1 hereunder in which a certificate shall

be revoked arises.

g) Pledging to CNNIC Trusted Network Service Center and stating to all certificate relying parties that within the usage period of the certificate, all the facts described in Section 1.3.2.1 are true.

h) Not using the certificate in transactions when a certificate subscriber knows that CNNIC Trusted Network Service Center may revoke the certificate according to this CPS or the certificate subscriber has filed an application for revocation or CNNIC Trusted Network Service Center is planning to revoke the certificate according to this CPS and has notified the certificate subscriber of it.

i) Immediately notifying the certificate relying parties engaged in any transaction to be completed at the time and clearly notifing that the certificate used in such transaction has to be revoked (through application by CNNIC Trusted Network Service Center or the certificate subscribers) and the certificate relying parties may not trust the certificate in the transaction when the certificate subscribers knows that CNNIC Trusted Network Service Center may revoke the certificate according to this CPS or the certificate subscribers has filed an application for revocation or CNNIC Trusted Network Service Center is planning to revoke the certificate according to this CPS and has notified the certificate subscribers of it.

j) The use of the certificate shall be limited to legal purposes and shall meet the related certificate policies and this CPS (or other released business proceedings). If the registrar has reason to believe that the private key corresponding to the public key used in the certificate has the danger of being disclosed, it shall notify in time CNNIC Trusted Network Service Center of revoking the certificate.

k) The certificate subscriber acknowledges that if it has not performed its obligations according to the provisions in the above terms, he shall bear liabilities for compensating the losses that may be incurred to CNNIC Trusted Network Service Center or its relying parties.

2.1.5 Obligations of the relying parties

The certificate relying parties trusting the digital certificates of CNNIC Trusted Network Service Center shall be responsible for:

a) Trusting a certificate after considering all the factors and ensuring that the certificate is reasonable.

b) Ensuring that the certificate to be used meets the purposes stipulated in this CPS before trusting this certificate, that is, trusting only the certificates issued by CNNIC Trusted Network Service Center as domain name certificates.

c) Checking the certificate status on the Certificate Revocation List (CRL) before trusting a certificate.

d) Implementing all the appropriate certificate path verification procedures.

e) Their trust of the certificate shows that they agree to accept the terms on limits of liability stipulated in this CPS.

2.2 Miscellaneous

2.2.1 Reasonable technology and disclaimer

CNNIC Trusted Network Service Center will adopt reasonable technology and management measures according to this CPS and exercise its rights and perform its obligations to the certificate subscribers and relying parties. CNNIC Trusted Network Service Center does not guarantee that the service provided according to this CPS will not be interrupted or have no error.

That is to say, though CNNIC Trusted Network Service Center or the Registration Authority representing CNNIC Trusted Network Service Center adopts reasonable technology and management measures when exercising its due rights and obligations according to this CPS, if the certificate subscribers or the relying parties suffer from debt, loss or damage by any nature arising out of the public key infrastructure or other related described in the CPS, each certificate subscriber shall agree that CNNIC

Trusted Network Service Center and the Registration Authority do not have to bear any liability, loss or damage.

Under the prerequisite that CNNIC Trusted Network Service Center or the Registration Authority representing CNNIC Trusted Network Service Center has adopted reasonable technology and management measures, if a certificate subscriber suffers from any loss or damage because it trusts any false or fabricated digital signature supported by a certificate issued by CNNIC Trusted Network Service Center held by another certificate subscriber, CNNIC Trusted Network Service Center or the Registration Authority representing CNNIC Trusted Network Service Center shall not be responsible for it.

Under the prerequisite that CNNIC Trusted Network Service Center has adopted reasonable technology and management measures to avoid or alleviate the consequences of uncontrollable events, if a certificate subscriber suffers from any adverse influence under circumstances that CNNIC Trusted Network Service Center cannot control, CNNIC Trusted Network Service Center shall not be responsible for it. The circumstances beyond the control of CNNIC Trusted Network Service Center include but not limited to the unavailability of the Internet or telecommunications or other infrastructure systems, or natural disasters, wars, military actions, national emergency, epidemic diseases, fire, flood, earthquake, strike or riots or the negligence or deliberate improper behaviors of other certificate subscribers or other third parties.

2.2.2 Limits of liability

2.2.2.1 Reasonableness of limits

Each certificate subscriber or relying party must agree that it is reasonable for CNNIC Trusted Network Service Center to limit their legal liability according to the conditions listed in the certificate subscriber's agreement and this CPS.

2.2.2.2 Limits of varieties of recoverable losses

If CNNIC Trusted Network Service Center violates the *Certificate Subscriber's Agreement* or has any duty-related responsibility, thus incurring any loss and damage to a certificate subscriber or a relying party, CNNIC Trusted Network Service Center shall not be liable for compensating for the loss and damage caused by the following causes:

a) any direct or indirect loss in profit or income, loss or damage in credit standing or business reputation, any loss of business opportunity, loss of project, or loss or inability to use any data, equipment or software;

b) Any loss or damage that is indirect, consequential or incidental.

2.2.2.3 Limit of amount

Even where CNNIC Trusted Network Service Center violates the *Certificate Subscriber's Agreement* or bears any duty-related responsibility, thus incurring any loss and damage to a certificate subscriber or a relying party, the legal liability that CNNIC Trusted Network Service Center shall assume for any certificate subscriber or any relying party shall be limited to no more than 10 times of each certificate's price for each domain name certificate under any circumstances.

2.2.2.4 Time limit for claiming compensation

If a certificate subscriber or a relying party claims compensation from the CNNIC, the cause incurring the claim of compensation shall be related to the issue or revocation of a certificate and shall be made within half a year from the date when the certificate subscriber or relying party knows this cause; or shall be made within half a year (if earlier) from the date when the cause is known. If the time limit of half a year expires, the claim for compensation must be given up and shall be absolutely forbidden.

2.2.2.5 Liabilities for deliberate improper behaviors

Any liabilities for deceit or deliberate improper behaviors shall not be within scope of any limit or disclaimer of this CPS, the certificate subscriber's agreement or the certificates issued by CNNIC Trusted Network Service Center.

2.2.2.6 Notice on the limits of certificate liability

CNNIC Trusted Network Service Center has given the following notice on limits of liability for the certificates it issues:

Employees in CNNIC Trusted Network Service Center issue this certificate as a Certificate Authority in accordance with the related regulations, when conditions apply to this certificate and according to the terms in the CPS signed by CNNIC Trusted Network Service Center.

Therefore, every person should read the Certificate Practice Statement that applies to domain name certificates (may browse http://tns.cnnic.cn) before trusting this certificate. The law of the People's Republic of China applies to this certificate, and the relying parties shall acknowledge that any dispute or problem arising out of trusting this certificate shall be governed by the law of the People's Republic of China.

A relying party shall not trust this certificate if it does not accept the terms and conditions used to issue this certificate.

CNNIC Trusted Network Service Center issues this certificate but does not have to bear any liability or duty-related responsibility to the relying parties.

Before trusting this certificate, a relying party shall make sure that the trusting act is fair, reasonable and without malice. Only in this way this certificate can be trusted;

Before trusting this certificate, a relying party shall determine that the use of the certificate is indeed appropriate in terms of the guaidlines stipulated in the CPS;

Before trusting this certificate, a relying party shall check the status of this certificate according to the Certificate Revocation List (CRL) and go through all the proper

certificate path verification procedures.

Though CNNIC Trusted Network Service Center has adopted reasonable technology and management measures, if there is still inaccuracy or misleading points in any aspect in this certificate, CNNIC Trusted Network Service Center shall not bear any liability for any loss or damage of the relying parties.

If there is inaccuracy or misleading points in any aspect of this certificate, and this kind of inaccuracy or misleading points are caused by the negligence of CNNIC Trusted Network Service Center, CNNIC Trusted Network Service Center may pay 10 times of each certificate's price at most to each relying party for the confirmed losses incurred by trusting this kind of inaccuracy or misleading points in this certificate, only that this kind of loss does not belong to or include (1) any direct or indirect loss, including profit or income loss, loss or damage in credit standing or business reputation, loss of business opportunity or chance, loss of project, loss or inability to use any data, equipment or software etc.; (2) any loss or damage that is indirect, consequential or incidental. Under such conditions, the credit limit applying to this certificate is 10 times of each certificate's price.

If a certificate subscriber or a relying party claims compensation from the CNNIC, the cause for the claim for compensation shall be related to the issue or revocation of a certificate, and the claim shall be made within half a year from the date when the certificate subscriber or relying party knows this cause; or shall be made within half a year (if earlier) from the date when the cause is known. When the time limit of half a year expires, the claim for compensation must be given up and shall be absolutely forbidden.

If this certificate includes any deliberate or reckless fraudulent statement made by CNNIC Trusted Network Service Center, this certificate does not make any limit to the legal liability that the relying party who suffers from loss for reasonably trusting the fraudulent statement of this statement shall bear.

The limit of legal liability described herein does not apply to personal injury or death (properablely can not occur)."

2.2.3 Liability that CNNIC Trusted Network Service Center assumes for digital certificates that have been accepted but have defects

If a certificate subscriber discovers, after accepting a certificate, that due to an error of the private key or public key included in the certificate, transactions based on the public key infrastructure cannot be properly completed or cannot be completed at all, the certificate subscriber shall immediately notify CNNIC Trusted Network Service Center of the case so as to revoke the certificate and reissue it. Or if a certificate subscriber discovers this condition within three (3) months after accepting the certificate and the certificate subscriber no longer needs the certificate, the certificate subscriber may apply for refunding provided that the CNNIC approves of it. If a certificate subscriber does not notify the CNNIC of this kind of error until three months later, the fees the certificate subscriber has submitted will not be refunded.

2.2.4 Certificate subscribers' transfer

A certificate subscriber may not transfer the rights endowed in the certificate subscriber's agreement or the certificate, and any transfer shall be invalid.

2.2.5 Authority of statement

Unless authorized by CNNIC Trusted Network Service Center, the agent or working personnel of CNNIC Trusted Network Service Center shall have no right to make any statement on the meaning or explanation of this CPS on behalf of CNNIC Trusted Network Service Center.

2.2.6 Alteration

CNNIC Trusted Network Service Center shall have right to alter this CPS, without having to give a notice in advance (see Section 2.2.8). No modification or alteration

may be carried out on the certificate subscriber's agreement, unless the provisions on modification or alteration in this CPS are met, or the definite written approval of CNNIC Trusted Network Service Center is obtained.

2.2.7 Preservation of ownership

The substantive right, copyright and intellectual property right of all the information on the certificate issued according to this CPS shall be owned by CNNIC Trusted Network Service Center.

2.2.8 Conflicts of terms

If the CPS conflicts with the certificate subscriber's agreement or other rules, directions or agreements, the certificate subscriber, the relying party and CNNIC Trusted Network Service Center must be restricted by the terms of this CPS, unless such terms are forbidden by law.

2.2.9 Fiduciary relationship

CNNIC Trusted Network Service Center or the Registration Authority representing CNNIC Trusted Network Service Center is not an agent or other representative of the certificate subscribers or the relying parties. The certificate subscribers or the relying parties shall not be entitled to bind, with an agreement or other forms, CNNIC Trusted Network Service Center or the Registration Authority representing CNNIC Trusted Network Service Center to be an agent of the certificate subscribers or the relying parties or bear the responsibilities of other representatives.

2.2.10 Cross certification

CNNIC Trusted Network Service Center shall preserve the right to carry out cross certification with other Certificate Authorities by defining and determining proper reasons.

According to the agreement of CNNIC and Entrust, CNNIC intermediate root CNNIC SSL is trusted by Entrust root certificate also. The domain certificates issued by CNNIC Trusted Network Service Center may be generated through different route either by CNNIC root or by Entrust root.

2.3 Interpretation and execution (governing law)

2.3.1 Governing law

This CPS is governed by the law of the People's Republic of China.

2.3.2 Terms that can be terminated and modified

If any term in this CPS is declared illegal, unenforceable or invalid, any illegal vocabulary in the terms shall be deleted until such terms become legal and enforceable, and the original meaning of such term shall be preserved. The unenforceability of any term in this CPS will not compromise the enforceability of any other terms.

The division or combination of CNNIC Trusted Network Service Center may lead to changes in its scope of operation, management and operation conditions. In this case, this CPS may also have to be altered. The change in operation activities will be consistent with the alteration of the CPS.

2.3.3 Procedure of dispute settlement

If a dispute between the interested parties cannot be settled through friendly consultation, the dispute shall be submitted to the China lnternational Economic and Trade Arbitration Commission for arbitration. The arbitral award is final and binding upon both parties. The course of arbitration shall be recorded in Chinese and the arbitral award shall be enforced by a court with jurisdiction.

2.4 Certificate charges

2.4.1 Certificate

The registration, renewal, reissue of SSL certificates (including single domain certificates, wildcard domain certificates, and multi-domain certificates)、DQ certificates (including single domain certificates and multi-domain certificates) and change of domain names of multi-domain certificates are paid services. The fees are determined according to regulations of the market and the management department.

2.4.2 Inquiry

Inquiry of certificates in CNNIC Trusted Network Service Center is a free service at present.

2.4.3 Revocation

Revocation of certificates in CNNIC Trusted Network Service Center is a free service at present.

2.4.4 Policy for refunding

Certificate charges of CNNIC Trusted Network Service Center will not be refunded after a certificate is issued.

2.4.5 Other charges

CNNIC Trusted Network Service Center temporarily does not charge except for certificate registration, renewal, reissue and change of domain names of multi-domain certificates.

2.5 Publicized information and repository

This article is the Certificate Practice Statement (CPS) of CNNIC Trusted Network Service Center and is published on the website of CNNIC Trusted Network Service Center, which is:

http://www.cnnic.cn

CNNIC Trusted Network Service Center maintains a repository, including the latest Certificate Revocation List (CRL) issued by root and intermediate root, the intermediate root certificate and root certificate of CNNIC Trusted Network Service Center, one copy of this CPS, CNNIC Trusted Network Service Center Certificate Policy (CP), and other related information. Except at most four hours of regular maintenance every week and emergency maintenance, the repository is open 24 hours every day and seven days every week. The repository of CNNIC Trusted Network Service Center may be access through the following URL:

http://www.cnnic.cn

All the Internet users are allowed to access publicized information and the repository but only the administrator of CNNIC Trusted Network Service Center is allowed to update them.

2.5.1 Control of certificate repository

The repository can be accessed online and unauthorized revision can be prevented.

2.5.2 Requirement on access to certificate repository

Only authorized working personnel of CNNIC Trusted Network Service Center can enter the repository to update and revise contents.

2.5.3 Updating cycle of certificate repository

The Certificate Revocation List (CRL) issued by intermediate root of the repository of

CNNIC Trusted Network Service Center is updated every 12 hours.

CRL issued by root will be renewed evey half a year (182 days), if there is no revocation of intermediate root. And CRL of root will be renewed immediately when intermediate root are revoked.

Other contents in the repository are changed at any moment according to changes.

2.6 Compliance evaluation

According to the provisions of the related law of the People's Republic of China, compliance evaluation presided by an independent external auditing agency shall be carried out at least once every twelve (12) months to check whether the systems in CNNIC Trusted Network Service Center that issue and revoke certificates and release Certificate Revocation List (CRL) strictly follow this CPS and the related control measures of CNNIC Trusted Network Service Center.

Auditing contents include:

a) Publicized business items

b) Completeness of services (including control of key management and management of the life cycle of certificates)

c) Environmental control

The audit results shall be reported to the Security Management Committee of CNNIC Trusted Network Service Center, which will arrange with CNNIC Trusted Network Service Center to determine improvement plans and adopt improvement actions according to the specific auditing opinions.

2.7 Confidentiality

Confidential information includes:

a) The signature keys of the certificate subscribers are confidential and are not provided to CNNIC Trusted Network Service Center

b) Information especially for the operation and control of CNNIC Trusted

Network Service Center is kept confidential by CNNIC Trusted Network Service Center; unless otherwise provided by law, such information shall not be disclosed.

c) Related information about the certificate subscribers other than the information publicized on the certificates, CRL, certificate policy and CPS is confidential information; unless required in the certificate policy or otherwise provided by law, and such information shall not be disclosed.

d) Generally speaking, the auditing results every year shall be kept confidential, unless the Security Management Committee of CNNIC Trusted Network Service Center deems it necessary to publicize the auditing results.

Non-confidential information includes:

a) Information included in the certificates signed by CNNIC Trusted Network Service Center and in the CRL is non-confidential information.

b) The information (other publicized business items) in the CPS publicized by CNNIC Trusted Network Service Center is non-confidential information.

c) When CNNIC Trusted Network Service Center revokes a certain certificate, the CRL lists the reasons for revoking the certificate. The code of the cause for revocation is non-confidential information and other certificate subscribers and certificate relying parties may share this information. However, other details concerning revocation are not publicized generally.

CNNIC Trusted Network Service Center will publicize information upon the law enforcement requirements of law enforcing personnel according to the provisions of law.

CNNIC Trusted Network Service Center will publicize the information of the related information holders to other parties upon the requirements of the information holders.

3 Identification and Authentication

3.1 Structure of CNNIC CA ROOT
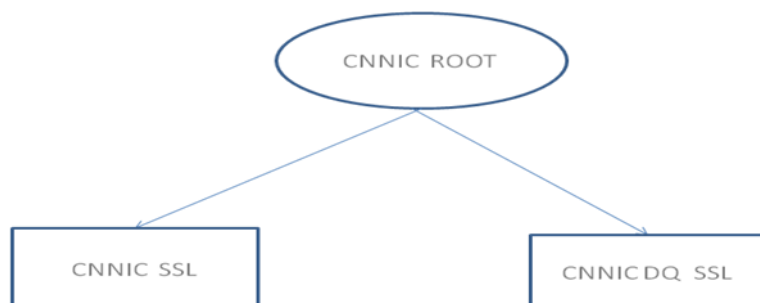
CNNIC ROOT is the root certificate, CNNIC SSL is the intermediate root certificate of the advanced certificate, CNNIC DQ SSL is the intermediate root certificate of domain quick certificate.

3.2 Naming and the first registration of SSL Certificates

3.2.1 Types of names

According to different types of corresponding entities of certificates, the entity names of the certificates issued by CNNIC Trusted Network Service Center may be single domain name or many domain names. Naming meets the X.500 regulations on distinguished names.

The issuer and subject field of the certificates issued by CNNIC Trusted Network Service Center include X.500 distinguished names. The subject distinguished names of the certificates issued by CNNIC Trusted Network Service Center are composed of the following contents:

Subject distinguished name of the root certificate of CNNIC Trusted Network Service Center

- Country (C) = CN
- Organization (O) = CNNIC
- Common name (CN) = CNNIC ROOT

Subject distinguished name of the intermediate root certificate of CNNIC Trusted

Network Service Center

- Country (C) = CN

- Organization (O) = Names of certificate holders

- Common name (CN)　= CNNIC SSL

The subject field of the domain name certificates includes an X.500 distinguished name, which is composed of the following contents:

- Country (C) = CN

- Organization (O) = CNNIC SSL

- Organization unit (OU)=SingleDomain (Single domain certificate or Wildcard domain certificate) or MultiDomain (Multi-domain certificates)

- Common name (CN) = This feature includes

Single domain name (Single domain certificate or Wildcard domain certificate), or many domain names (Multi-domain certificates)

3.2.2 Requirements on names

The names included in the certificates issued by CNNIC Trusted Network Service Center shall be composed of the domain names or the serial number automatically generated by CNNIC Trusted Network Service Center and the fixed contents of the certificates of CNNIC Trusted Network Service Center.

3.2.3 Applicants' anonymity or pseudonym

Applicants cannot apply for a certificate anonymously or with a pseudonym, and no anonymity or pseudonym can be used in a certificate.

3.2.4 Rules on understanding different forms of names

Interpret according to the rules on naming of X.500 distinguished names.

3.2.5 Uniqueness of names

The subject distinguished name of the certificate issued by CNNIC Trusted Network Service Center to a certain entity is unique in the trust domain of CNNIC Trusted Network Service Center.

3.2.6 Identification, authentication and role of trademarks

The subject distinguished name of the certificates issued by CNNIC Trusted Network Service Center is only related to domain names and certificate holders' names, but not related to trademarks.

3.2.7 Settlement of disputes on names

Disputes on names shall be settled by CNNIC Trusted Network Service Center according to specific conditions.

3.2.8 First registration of SSL Certificates

3.2.8.1 Single domain and wildcard domain certificates

1. The certificate application commissioner submits the application materials to the inputer at a Local Registration Authority (LRA):

For an independent server (the server to be installed with a certificate is managed by the certificate applicant, the same hereunder), the application materials shall include the following documents:

> ➢ Proof of identification of the certificate applicant:
>> ■ Enterprises shall provide: photocopy of the organization code certificate or photocopy of the enterprise legal person business license (each page affixed with an official seal);
>> ■ Government departments shall provide: photocopy of the organization code certificate (each page affixed with an official seal);

- ■ Institutions shall provide: photocopy of the organization code certificate (each page affixed with an official seal);

- ■ Social organizations shall provide: photocopy of the organization code certificate (each page affixed with an official seal).

- ■ Natural persons shall provide: photocopy of valid personal identification.

➢ Original of the application for certificate registration.

➢ When the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

As for managed servers (servers to be installed with a certificate are managed by another agency entrusted by the certificate applicant, the same hereunder), the certificate applicant shall be handled by the entrusted agency on behalf, and the application materials shall include the following documents:

➢ Proof of the identity of the certificate applicant.

- ■ Enterprises shall provide: photocopy of the organization code certificate or photocopy of the enterprise legal person business license (each page affixed with an official seal);

- ■ Government departments shall provide: photocopy of the organization code certificate or photocopy of the government department legal person certificate (each page affixed with an official seal);

- ■ Institutions shall provide: photocopy of the organization code certificate or photocopy of the institution legal person certificate (each page affixed with an official seal);

- ■ Social organizations shall provide: photocopy of the organization code certificate or photocopy of the social organization legal person registration certificate (each page affixed with an official seal).

- ■ Natural persons shall provide: photocopy of valid personal identification.

➢ Original of the application for certificate registration.

➢ Photocopy of the proof of the identity of the commissioner of the entrusted agency.

➢ When the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of

the director shall be submitted.

2. The inputer at the Local Registration Authority carries out preliminary examination. Through the domain name registration information inquiry (whois), the inputer gets the information of the domain name registrar of the domain name certificate application, checks whether the domain name registrar is consistent with the domain name certificate applicant, and determines whether the domain name certificate applicant indeed has this domain name through preliminary examination.

3. After the preliminary examination is passed, the inputer at the Local Registration Authority puts in the above information through the RA system, submits it for application, and passes on all the paper application materials to the RA auditor at the CNNIC Registration Authority with a safe method. If the preliminary examination is not passed, the domain name certificate applicant is required to re-apply after the change of information of the domain name registrar.

4. The RA auditor checks whether the legal domain name subscriber is consistent with the certificate applicant (also using the whois function), and whether the information is true, and compares it with the application information in the RA system. The RA auditor confirms the information with the director and the commissioner respectively through telephone.

5. If the confirmation is passed, the RA auditor logs on the RA system, approves the certificate application, emails the 16 numbers of the reference number and authorization code to commissioner If the confirmation is not passed, the certificate registration application is rejected and all the materials are returned to the Local Registration Authority, attached with reasons for rejection. The Local Registration Authority contacts the application commissioner, who carries out corresponding revision according to the reasons for rejection and re-applies.

3.2.8.2 Multi-domain certificates

1. The certificate application commissioner submits the application materials to the

inputer at the Local Registration Authority (LRA):

As for independent servers, the application materials shall include the following documents:

- Proof of identification of the certificate applicant:
  - Enterprises shall provide: photocopy of the organization code certificate or photocopy of the enterprise legal person business license (each page affixed with an official seal);
  - Government departments shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - Institutions shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - Social organizations shall provide: photocopy of the organization code certificate (each page affixed with an official seal).
  - Natural persons shall provide: photocopy of valid personal identification.
- Original of the application for certificate registration.
- When the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

As for managed servers, the application materials shall include the following documents:

- Proof of the identity of all the certificate applicants.
  - Enterprises shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - Government departments shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - Institutions shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - Social organizations shall provide: photocopy of the organization code certificate (each page affixed with an official seal).
  - Natural persons shall provide: photocopy of valid personal identification.
- Original of the application for certificate registration.
- Photocopy of the proof of the identity of the commissioner of the entrusted

agency.

➢ When the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

2. The inputer at the Local Registration Authority carries out preliminary examination. Through the domain name registration information inquiry (whois), the inputer gets the information of all the domain name registrars of the multi-domain certificate application, checks whether the domain name registrars are consistent with the domain name certificate applicants, and determines whether the domain name certificate applicants indeed have this domain name through preliminary examination.

3. After the preliminary examination is passed, the inputer at the Local Registration Authority puts in the above information through the RA system, submits it for application, and passes on all the paper application materials to the RA auditor at the CNNIC Registration Authority via a safe method. If the preliminary examination is not passed, that is, a certain domain name applicant is inconsistent with a domain name registrars, the domain name certificate applicant is required to change the information of the domain name registrar before the entrusted agency re-applies for a multi-domain certificate or the domain name with inconsistent information is deleted from the multi-domain certificate.

4. The RA auditor checks whether the legal domain name subscriber is consistent with the certificate applicant (also using the whois function), and whether the information is true, and compares it with the application information in the RA system. The RA auditor confirms the information with the director and the commissioner respectively through telephone.

5. If the confirmation is passed, the RA auditor will log on the RA system, approve the certificate application, emails the 16 numbers of the reference number and authorization code to commissioner. If the confirmation is not passed, the certificate registration application will be rejected and all the materials will be returned to the Local Registration Authority, attached with reasons for rejection.

The Local Registration Authority will contact the application commissioner, who will carry out corresponding revision according to the reasons for rejection and re-applies.

3.3 Naming and the first registration of DQ Certificates

3.3.1 Types of names

According to different types of the installation belongs to corresponding domain of certificates, the names of the certificates issued by CNNIC Trusted Network Service Center may be single domain name or many domain names. Naming meets the X.500 regulations on distinguished names.

The issuer and subject field of the certificates issued by CNNIC Trusted Network Service Center include X.500 distinguished names. The subject distinguished names of the certificates issued by CNNIC Trusted Network Service Center are composed of the following contents:

Subject distinguished name of the root certificate of CNNIC Trusted Network Service Center

- Country (C) = CN
- Organization (O) = CNNIC
- Common name (CN) = CNNIC ROOT

Subject distinguished name of the intermediate root certificate of DQ certificate of CNNIC Trusted Network Service Center

- Common name (CN)　= CNNIC DQ SSL
- Organization (O) = CNNIC
- Country (C) = CN

The subject field of the DQ certificates includes an X.500 distinguished name, which is composed of the following contents:

- Country (C) = CN
- Organization (O) = This feature includes Single domain(Domain field of Single domain certificate or the first Domain field of Multi-domain certificates)

- Organization unit (OU)= Domain-Quick SSL

- Common name (CN) = This feature includes Single domain name (Single domain certificate), or Multi-domain names (Multi-domain certificates)

3.3.2 Requirements on names

The names included in the Domain Quick certificates issued by CNNIC Trusted Network Service Center shall be composed of the domain names and the fixed contents of the certificates of CNNIC Trusted Network Service Center.

3.3.3 Applicants' anonymity or pseudonym

Applicants cannot apply for a certificate anonymously or with a pseudonym, and no anonymity or pseudonym can be used in a certificate. Only domain name will be displayed in certificate.

3.3.4 Rules on understanding different forms of names

Interpret according to the rules on naming of X.500 distinguished names.

3.3.5 Uniqueness of names

The subject distinguished name of the certificate issued by CNNIC Trusted Network Service Center to a certain entity is unique in the trust domain of CNNIC Trusted Network Service Center.

3.3.6 Identification, authentication and role of trademarks

The subject distinguished name of the certificates issued by CNNIC Trusted Network Service Center is only related to domain names, but not related to trademarks.

3.3.7 Settlement of disputes on names

Disputes on names shall be settled by CNNIC Trusted Network Service Center according to specific conditions.

3.3.8 First registration of DQ Certificates

3.3.8.1 Single domain and Multi-domain certificates

commissionercommissionercommissionerA. The certificate application commissioner submits the application materials to the entry clerk at the Local Registration Authority (LRA). In the event that the applicant is a user of ".CN" or "中国" domain name that passed CNNIC domain name registration audit, the domain name application materials are deemed as domain quick (DQ) certificate application materials, and the domain name that passed the audit of CNNIC real-name system is deemed as in compliance with the audit of DQ certificate application materials.

When auditing registration application for ".CN" or "中国" domain names, CNNIC may examine the identity of the application commissioner and the business license or organization code certificate.

1. The certificate applicant shall provide the following materials to the reception authority (RA):

> ➢ Confirmation of e-application, including application agreement;

2. After the application is submitted by the user, the Local Reception Authority (LRA) will carry out preliminary examination over the materials submitted, and then upload the application information of the user into CNNIC WebRA system, and the system will automatically judge whether the domain name applied for is a ".CN" or "中国" domain name, and determine:

> ➢ **Whether the domain name holder has passed the real-name contact authentication, i.e. whether the user is on the white list;**
> ➢ **Whether the domain name has passed the examination;**
> ➢ **Whether the name of company who applies for the domain name is consistent with that of the returned domain name;**
> ➢ **Whether the phone number provided at the time of registration is consistent with the returned result of the white list.**

3. The application will not be approved unless the above 4 requirements are satisfied simultaneously;

4. Upon the approval of the application, the system will send the DQ certificate registration link to the commissioner; in case of failure of achieving the approval, the

system will reject the certificate registration application, and inform the user of the reason.

5. After logon through the certificate registration link provided, the commissioner is required to validate the ownership of the domain name; the system will send an email of validation registration certificate to the registrant, and the user can perform validation by clicking the link provided in the email. The certificate will not be downloaded until successful validation, and the certificate will not be issued in case of failure of validation.

B. In case of ".CN" or "中国" domain name or any other type of domain name that failed to achieve CNNIC real-name authentication, application should be performed in accordance with the following procedures.

1. The certificate applicant shall submit the following materials to the LRA:

> Confirmation of e-application, including application protocols;

> Photocopy of the commissioner's ID card;

> Photocopy of business license (bearing the official seal) or organization code certificate (bearing the official seal).

2. The entry clerk at the LRA carries out preliminary examination. Through whois function, the entry clerk gets the information of the domain name registrant of the domain name certificate application, and checks whether the domain name registrant is consistent with the domain name certificate applicant, and carries out preliminary examination to confirm the domain name certificate applicant indeed holds such domain name.

3. After preliminary examination, the entry clerk at the LRA will upload the above information into RA system, submit the application, and transfer all the paper application materials to the RA auditor at the CNNIC Registration Authority with a safe method. In case of failure of passing the preliminary examination at the LRA, the domain name certificate applicant is required to re-apply after modification of information of the domain name registrant.

4. The RA auditor checks whether the legal domain name holder is consistent with the certificate applicant (also using the whois function), and whether the information is

authentic, and compares it with the application information in the RA system.

5.   After the auditor approves the application, the system will send the link for DQ certificate registration to the commissioner; in case of failure of passing the system audit, the application for certificate registration will be rejected, and the user will be informed of the reason.

6.   After logon through the certificate registration link, the system needs to verify the domain name ownership; and the system will send a validation email to the domain name holder, and the user can validate it by clicking the link provided in the email. The certificate will not be downloaded until successful validation, and the certificate will not be issued in case of failure of validation.

3.4Method for proving the possession of a private key

CNNIC Trusted Network Service Center verifies that a certificate applicant has a private key corresponding to the certificate public key by using the certificate request in PKCS#10 attached with a digital signature.

4 Operation Codes

4.1 Issuing of certificates under CNNIC ROOT certificate chain

There are two types of issuing of certificates under CNNIC ROOT certificate chain: SSL certificates and DQ certificates. And these two kinds of certificates have the same business processes of certificate freezing、certificate renewing and certificate releasing in the certificate issued center CNNIC CA, and other aspects of SSL certificates and the DQ certificate have some differents, is reflected in different chapters.

4.2 Application, issue, acceptance, revocation and release of SSL Certificates

4.2.1 Certificate application

4.2.1.1 Processing of application

The commissioners for applying for SSL certificates must go to a Local Registration Authority of CNNIC Trusted Network Service Center designated by the CNNIC to submit applications. CNNIC Trusted Network Service Center (including the Registration Authority) does not accept applications directly from applicants.

4.2.1.2 Verification of identity

Documents used to prove the certificate subscriber organizations, commissioners and identity of commissioners are explained in Section 3.2 of this CPS, and applicants shall carry out application operations according to Section 3.2 of this CPS. After the Registration Authority of CNNIC Trusted Network Service Center completed the

procedure of verifying identity, it emails the first 16 numbers of the reference number and authorization code to commissioner.

4.2.2 Issuing and acceptance of certificates

4.2.2.1 Single domain and wildcard domain certificates

The steps for issuing and accepting single domain and wildcard domain certificates are as follows:

1. The certificate application commissioner generates a certificate request CSR in the Web server.

2. The certificate application commissioner accesses the CNNIC certificate download page, submits the CSR and puts in the reference number and the authorization code.

3. CNNIC Trusted Network Service Center system automatically checks the completeness of the CSR.

4. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner downloads it and then installs it.

5. The completion of CNNIC Trusted Network Service Center's issuing of a certificate shows that the applicant accepts the services of CNNIC Trusted Network Service Center.

4.2.2.2 Multi-domain certificates

The steps for issuing and accepting multi-domain certificates are as follows:

1. The certificate application commissioner generates a certificate request CSR in the Web server.

2. The certificate application commissioner accesses the CNNIC certificate download page, submits the CSR and puts in the reference number and the authorization code.

3. CNNIC Trusted Network Service Center system automatically checks the completeness of the CSR.

4. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner downloads it and then installs it.

5. The completion of CNNIC Trusted Network Service Center's issuing of a certificate shows that the applicant accepts the services of CNNIC Trusted Network Service Center.

4.2.3 Publication of certificates

The domain name certificates issued by CNNIC Trusted Network Service Center are not published in the repository, but users could check domain name certificates registry information through CNNIC Trusted Network Service Center's website.

4.2.4 Reissue of SSL Certificates

In the certificate system of CNNIC Trusted Network Service Center, the reissue of certificates requires the generation of another certificate request CSR, and CNNIC Trusted Network Service Center requires the use of a key pair different from the original key pair to apply and the use of the old certificate request document is not allowed.

After the reissue of a new certificate, the original certificate becomes invalid immediately, and the usage period of the new certificate is the same with the original certificate.

4.2.4.1 **Reissue of the single domain and wildcard domain certificates**

1. The certificate application commissioner submits the application materials to the inputer at the Local Registration Authority (LRA):

For independent servers, the application materials include the following documents:

➢ Original of the application for reissue of certificate.

➢ When the certificate applicant is a natural person, the photocopy of valid

personal identity certification shall be submitted; when the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

For managed servers, the application materials shall include the following documents:

➢ Original of the application for reissue of certificate.

➢ Photocopy of the identity certification of the commissioner of the entrusted agency.

2. The inputer at the Local Registration Authority puts in the above information via the RA system and submits the application.

3. The inputer at the Local Registration Authority passes on all the application materials to the RA auditor at the CNNIC Registration Authority with a safe method.

4. The RA auditor checks the materials and compares the application information in the RA system with the original registration information of the domain name certificate. The RA auditor confirms the information with the director (if any) and the commissioner respectively through telephone.

5. If the confirmation is passed, the RA auditor logs on the RA system, approves the certificate application, emails the 16 numbers of the reference number and authorization code to commissioner. If the confirmation is not passed, the application for the reissue of a certificate is rejected and all the materials are returned to the Local Registration Authority, attached with reasons for rejection. The Local Registration Authority contacts the application commissioner, who carries out corresponding revision according to the reasons for rejection and re-applies for reissue.

6. commissionerThe certificate application commissioner generates a certificate request CSR in the Web server.

7. The certificate application commissioner accesses the CNNIC certificate download page, submits the CSR and puts in the reference number and the authorization code.

8. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner installs it.

4.2.4.2 Reissue of multi-domain certificates

1. The certificate application commissioner submits the application materials to the inputer   at the Local Registration Authority (LRA):

For independent servers, the application materials include the following documents:

➢ Original of the application for reissue of certificate.

➢ When the certificate applicant is a natural person, the photocopy of valid personal identity certification shall be submitted; when the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

For managed servers, the application materials shall include the following documents:

➢ Original of the application for reissue of certificate.

➢ Photocopy of the identity certification of the commissioner of the entrusted agency.

2. The inputer at the Local Registration Authority puts in the above information via the RA system and submits the application.

3. The inputer at the Local Registration Authority passes on all the application materials to the RA auditor at the CNNIC Registration Authority with a safe method.

4. The RA auditor checks the materials and compares the application information in the RA system with the original registration information of the domain name certificate. The RA auditor confirms the information with the director (if any) and the commissioner respectively through the telephone.

5. If the confirmation is passed, the RA auditor logs on the RA system, approves the certificate application, emails the 16 numbers of the reference number and authorization code to commissioner. If the confirmation is not passed, the application for the reissue of a certificate is rejected and all the materials are returned to the Local

Registration Authority, attached with reasons for rejection. The Local Registration Authority contacts the application commissioner, who carries out corresponding revision according to the reasons for rejection and re-applies for reissue.

6. The certificate application commissioner generates a certificate request CSR in the Web server.

7. The certificate application commissioner accesses the CNNIC certificate download page, submits the CSR and puts in the reference number and the authorization code.

8. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner installs it.

4.2.5 Renewal and annual audit of SSL Certificates

When a certificate subscriber's certificate expires, the certificate subscriber shall acquire a new certificate to maintain the continuity of the use of the certificate. The certificate subscriber generates a new key pair to replace the expired key pair, which is called "key renewal". However, in some cases, the certificate subscriber hopes to apply for a new certificate for the existing key pair, which is called "certificate renewal".

In the certificate system of CNNIC Trusted Network Service Center, the renewal of a certificate requires the certificate subscriber to generate another certificate request document CSR, and at the same time, CNNIC Trusted Network Service Center requires the certificate subscriber to use a key pair different from the original key pair to apply, and the use of the old certificate request document CSR is not allowed (that is, "key renewal" must be carried out).

The certificate renewal period is within three months before the current certificate becomes invalid. Before or after this period, CNNIC Trusted Network Service Center will reject the application for renewal.

After the renewal, the new certificate shall be immediately installed after being downloaded. The period of validity of the renewal is postponed accordingly, that is

the period before the new certificate becomes invalid = current time + the length of time for the newly purchased certificate + the length of remaining time of the current certificate.

4.2.5.1Renewal of single domain and wildcard domain certificates

1. The certificate application commissioner submits the application materials to the inputer at the Local Registration Authority (LRA):

For independent servers, the application materials include the following documents:

- ➢ Proof of the identity of the certificate applicant:
  - ■ Enterprises shall provide: photocopy of the organization code certificate or photocopy of the enterprise legal person business license (each page affixed with an official seal);
  - ■ Government departments shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - ■ Institutions shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - ■ Social organizations shall provide: photocopy of the organization code certificate (each page affixed with an official seal).
  - ■ Natural persons shall provide: photocopy of valid personal identification.
- ➢ Original of the application for renewal of certificate.
- ➢ When the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

For managed servers, the application materials shall include the following documents:

- ➢ Proof of the identity of the certificate applicant.
  - ■ Enterprises shall provide: photocopy of the organization code certificate or photocopy of the enterprise legal person business license (each page affixed with an official seal);
  - ■ Government departments shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - ■ Institutions shall provide: photocopy of the organization code certificate (each page affixed with an official seal);

- ■ Social organizations shall provide: photocopy of the organization code certificate (each page affixed with an official seal).

- ■ Natural persons shall provide: photocopy of valid personal identification.

- ➢ Original of the application for renewal of certificate.

- ➢ Photocopy of the proof of the identity of the commissioner of the entrusted agency.

- ➢ When the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

2. The inputer at the Local Registration Authority puts in the above information via the RA system and submits the application.

3. The inputer at the Local Registration Authority passes on all the application materials to the RA auditor at the CNNIC Registration Authority with a safe method.

4. The RA auditor checks the materials and compares the application information in the RA system with the original registration information of the domain name certificate. The RA auditor confirms the information with the director (if any) and the commissioner respectively through telephone.

5. If the confirmation is passed, the RA auditor logs on the RA system, approves the certificate application, emails the16 numbers of the reference number and authorization code to commissione. If the confirmation is not passed, the application for the renewal of a certificate is rejected and all the materials are returned to the Local Registration Authority, attached with reasons for rejection. The Local Registration Authority contacts the application commissioner, who carries out corresponding revision according to the reasons for rejection and re-applies for renewal.

6.The certificate application commissioner generates a certificate request CSR in the Web server.

7. The certificate application commissioner accesses the CNNIC certificate download page, submits the CSR and puts in the reference number and the authorization code.

8. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner installs it.

4.2.5.2Renewal of multi-domain certificates

1. The certificate application commissioner submits the application materials to the inputer at the Local Registration Authority (LRA):

For independent servers, the application materials include the following documents:

- ➢ Proof of the identity of the certificate applicant:
  - ■ Enterprises shall provide: photocopy of the organization code certificate or photocopy of the enterprise legal person business license (each page affixed with an official seal);
  - ■ Government departments shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - ■ Institutions shall provide: photocopy of the organization code certificate (each page affixed with an official seal);
  - ■ Social organizations shall provide: photocopy of the organization code certificate (each page affixed with an official seal).
  - ■ Natural persons shall provide: photocopy of valid personal identification.
- ➢ Original of the application for renewal of certificate.
- ➢ When the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

For managed servers, the application materials shall include the following documents:

- ➢ Proof of the identity of all the certificate applicants.
  - ■ Enterprises shall provide: photocopy of the organization code certificate or photocopy of the enterprise legal person business license (each page affixed with an official seal);
  - ■ Government departments shall provide: photocopy of the organization code certificate or photocopy of the government department legal person certificate (each page affixed with an official seal);
  - ■ Institutions shall provide: photocopy of the organization code certificate or photocopy of the institution legal person certificate (each page affixed

with an official seal);

- Social organizations shall provide: photocopy of the organization code certificate or photocopy of the social organization legal person registration certificate (each page affixed with an official seal).

- Natural persons shall provide: photocopy of valid personal identification.

➢ Original of the application for reissue of certificate.

➢ Photocopy of the proof of the identity of the commissioner of the entrusted agency.

➢ When the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

2. The inputer at the Local Registration Authority puts in the above information via the RA system and submits the application.

3. The inputer at the Local Registration Authority passes on all the application materials to the RA auditor at the CNNIC Registration Authority with a safe method.

4. The RA auditor checks the materials and compares the application information in the RA system with the original registration information of the domain name certificate. The RA auditor confirms the information with the director and the commissioner respectively through telephone.

5. If the confirmation is passed, the RA auditor logs on the RA system, approves the certificate application, emails the 16 numbers of the reference number and authorization code to commissioner. If the confirmation is not passed, the application for the renewal of a certificate is rejected and all the materials are returned to the Local Registration Authority, attached with reasons for rejection. The Local Registration Authority contacts the application commissioner, who carries out corresponding revision according to the reasons for rejection and re-applies for renewal.

6. The certificate application commissioner generates a certificate request CSR in the Web server

7. The certificate application commissioner accesses the CNNIC certificate download page, submits the CSR and puts in the reference number and the authorization code.

8. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner installs it.

4.2.5.3 Types of Certificate on annual audit

annual audit of certificate is to ensure the validity of user information, application period for the extra 1-year certificate will implement the annual inspection system. Auditor will conduct an annual audit of the effectiveness of user information, the inspection process is same as the application process, but without requiring the user to submit the data, but by the CNNIC launched their own trusted network of service centers to the third party inspection.

4.2.6 Change of domain name in multi-domain certificates

CNNIC CA does not provide domain changes server of Mutli-domain certificate anymore.4.2.7 Revocation of certificates

4.2.7.1 Circumstances for revocation

In any of the following cases, CNNIC Trusted Network Service Center shall be entitled to revoke a domain name certificate that it has issued:

1. Discovering that there is false information in the materials provided by the certificate subscriber to apply for the domain name certificate;

2. The certificate subscriber fails to fulfill the obligations stipulated in the certificate subscriber's agreement;

3. The certificate subscriber requests the revocation of the domain name certificate;

4. The subject of the certificate subscriber disappears;

5. The certificate subscriber changes the purposes of the domain name certificate;

6. Other circumstances required by laws or regulations.

4.2.7.2 Procedure of revocation

If a circumstance other than the third item of Section 4.5.1 arises, CNNIC Trusted Network Service Center will automatically revoke the domain name certificate and notify the certificate subscriber.

The certificate subscriber also has the right to apply for revocation of a certificate and the process of applying for revocation is as follows:

4.2.7.3 Revocation of single domain and wildcard domain certificates

1. The certificate subscriber submits the application materials for revocation of paper certificate to the inputer at the Local Registration Authority (LRA).

    For independent servers, the application materials include:

    ➢ Original of the application for revocation of certificate.

    ➢ When the certificate applicant is a natural person, the photocopy of valid personal identity certification shall be submitted; when the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

    For managed servers, the application materials shall include:

    ➢ Original of the application for revocation of certificate.

    ➢ Photocopy of the proof of the identity of the commissioner of the entrusted agency.

2. The inputer at the Local Registration Authority puts in the above information via the RA system and submits the application.

3. The inputer at the Local Registration Authority passes on all the application materials to the RA auditor at the CNNIC Registration Authority with a safe

method.

4. The RA auditor checks the materials and compares the application information in the RA system with the original registration information of the domain name certificate. The RA auditor confirms the information with the director (if any) and the commissioner respectively through telephone.

5. If the examination is passed, the RA auditor directly revokes the domain name certificate. If the examination is not passed, the application for the revocation of certificate is rejected and all the materials are returned to the Local Registration Authority, attached with reasons for rejection. The Local Registration Authority contacts the application commissioner, who carries out corresponding revision according to the reasons for rejection and re-applies for revocation.

4.2.7.4 Revocation of multi-domain certificates

1. The certificate subscriber submits the application materials for revocation of paper certificate to the inputer at the Local Registration Authority (LRA).

   For independent servers, the application materials include:
   ➢ Original of the application for revocation of certificate.
   ➢ When the certificate applicant is a natural person, the photocopy of valid personal identity certification shall be submitted; when the certificate applicant is an enterprise/government department/institution/social organization, the photocopy of the identity of the director and commissioner shall be submitted.

   For managed servers, the application materials shall include:
   ➢ Original of the application for revocation of certificate.
   ➢ Photocopy of the proof of the identity of the commissioner of the entrusted agency.

2. The inputer at the Local Registration Authority puts in the above information via the RA system and submits the application.

3. The inputer at the Local Registration Authority passes on all the application materials to the RA auditor at the CNNIC Registration Authority with a safe method.

4. The RA auditor checks the materials and compares the application information in the RA system with the original registration information of the domain name certificate. The RA auditor confirms the information with the director (if any) and the commissioner respectively through telephone.

5. If the examination is passed, the RA auditor directly revokes the domain name certificate. If the examination is not passed, the application for the revocation of certificate is rejected and all the materials are returned to the Local Registration Authority, attached with reasons for rejection. The Local Registration Authority contacts the application commissioner, who carries out corresponding revision according to the reasons for rejection and re-applies for revocation.

4.2.7.5 Revocation of effectiveness

CNNIC Trusted Network Service Center releases the status of revocation on the Certificate Revocation List (CRL), and the effectiveness of a certain certificate will be terminated.

4.2.7.6 Entities that can request the revocation of a certificate

CNNIC Trusted Network Service Center or the certificate subscriber may request the revocation of a certificate under circumstances described in Section 4.5.1 of this CPS.

4.2.7.7 Process of request for revocation

When CNNIC Trusted Network Service Center has sufficient reason to believe that a certificate shall be revoked, the related personnel of the Certificate Authority or the Registration Authority of CNNIC Trusted Network Service Center may submit

request for revoking the certificate through a process determined internally. After the revocation of the certificate, CNNIC Trusted Network Service Center will notify the certificate subscriber of the revocation of the certificate and the reason for revocation with a proper method, including mail and fax etc.

The certificate subscriber may also request the revocation of its own certificate through the procedure of revocation. When the certificate subscriber submits a request for revocation, it shall also provide the materials provided for application for the certificate as the information for identification.

4.2.7.8Time limit for putting forward a request for revocation

When any of the cases in Section 4.5.1 of this CPS is discovered to arise, the time interval from the discovery of the need to revoke a certificate to putting forward the request for revocation shall not exceed 24 hours.

4.2.7.9Time limit for processing a request for revocation by CNNIC Trusted Network Service Center

The time between the receptions of a request for revocation (including paper materials) to the completion of the processing of the request by the Registration Authority (RA) of CNNIC Trusted Network Service Center shall not exceed two (2) working days. The working days of CNNIC Trusted Network Service Center do not include weekends or national holidays.

4.2.7.10Relying parties' requirement on checking the revocation of a certificate

Whether or not a relying party checks the revocation of a certificate is completely determined by the relying party's requirement on security.

4.2.7.11 CRL release frequency

The intermediate root of CNNIC Trusted Network Service Center issues one Certificate Revocation List (CRL) of intermediate root every twelve (12) hours. CRL issued by root will be renewed evey half a year (182 days), if there is no revocation of intermediate root. And CRL of root will be renewed immediately when intermediate root are revoked.

4.2.7.12 Maximum latency for CRL releasing

The latency for a domain certificate from its revocation to its being publicized on the CRL shall not exceed twelve (12) hours. CRL of the root will be renewed immediately when intermediate root is revoked.

4.2.7.13 Availability of certificates online status inquiry

CNNIC Trusted Network Service Center provides the online inquiry service for certificate status (OCSP). This service is available 7×24 hours every week except at most four (4) hours' regular maintenance and emergency maintenance.

4.2.7.14 Requirements on online status inquiry

Whether a relying party carries out online status inquiry is completely determined by the relying party's requirements on security. If a relying party has high requirements on security guarantee and completely relies on a certificate to carry out identification and authorization, the relying party may inquire about the status of a certificate via the certificate status online inquiry system.

4.2.7.15 Other forms for releasing information on revocation

At present, CNNIC Trusted Network Service Center only provides OCSP inquiry and CRL inquiry through the LDAP contents service and HTTP service.

4.2.7.16Special requirements on key damage

Whether a certificate subscriber or CNNIC Trusted Network Service Center, once discovering a certificate key suffers from security damage, shall immediately revoke the certificate.

4.3 Application, issue, acceptance, Revocation and release of DQ Certificates

4.3.1 Certificate application

4.3.1.1 Processing of application

The applicants that apply the DQ certificate through other business, the corresponding documents must be submitted to the designated locations, and must be submitted to the specified URL address of an application, CNNIC trusted network of service centers (including the registry) does not accept applications directly to the applicant.

4.3.1.2 Verification of identity

Documents used to prove the certificate subscriber organizations, commissioners and identity of commissioners are explained in Section 3.3 of this CPS, and applicants shall carry out application operations according to Section 3.3 of this CPS. After the Registration Authority of CNNIC Trusted Network Service Center completed the procedure of verifying identity, the user can download the certificate directly.

4.3.2 Issuing and acceptance of certificates

4.3.2.1 Single domain certificates

The steps for issuing and accepting single domain certificates are as follows:
1. The certificate application commissioner generates a certificate request CSR in the Web server.

2. The certificate application commissioner accesses the CNNIC certificate download page, submits the CSR.

3. CNNIC Trusted Network Service Center system automatically checks the completeness of the CSR.

4. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner downloads it and then installs it.

5. The completion of CNNIC Trusted Network Service Center's issuing of a certificate shows that the applicant accepts the services of CNNIC Trusted Network Service Center.

4.3.2.2 Multi-domain certificates

The steps for issuing and accepting multi-domain certificates are as follows:

1. The certificate application commissioner generates a certificate request CSR in the Web server.

2. The certificate application commissioner accesses the CNNIC certificate download page, submits the CSR.

3. CNNIC Trusted Network Service Center system automatically checks the completeness of the CSR.

4. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner downloads it and then installs it.

5. The completion of CNNIC Trusted Network Service Center's issuing of a certificate shows that the applicant accepts the services of CNNIC Trusted Network Service Center.

4.3.3 Publication of certificates

The domain name certificates issued by CNNIC Trusted Network Service Center are not published in the repository, but users could check domain name certificates registry information through CNNIC Trusted Network Service Center's website.

4.3.4 Reissue of DQ Certificates

In the certificate system of CNNIC Trusted Network Service Center, In the

certificate system of CNNIC Trusted Network Service Center, reissue of certificate can be classified into the following two circumstances:

1. The user certificate file is lost before installation;

2. The key information of the user is leaked.

Under these two circustmances:

the reissue of certificates requires the generation of another certificate request CSR, and CNNIC Trusted Network Service Center requires the use of a key pair different from the original key pair to apply and the use of the old certificate request document is not allowed.

After the reissue of a new certificate, the original certificate becomes invalid immediately, and the usage period of the new certificate is the same with the original certificate.

Restriction condition:

Users reissue Certificate by themselves and Certificate reissue is allowed at most 3 times a month.

4.3.4.1 Reissue of the single domain certificates

The applicants that apply the DQ certificate through other business:

1. The applicant fills out the application information and submits an application through the address that CNNIC URL specified.

2. During the period of validity of the certificate, after the user submits the application, the system will automatically detect whether the information submitted is the correct information. If the information of application consistent with the original message (mostly commissioner's information, company information, etc.), this reissue application will be approved , if the application of certificate is valid for more than one-years, will be rigorous audit conducted at the annual inspection.

3. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner installs it.

4.3.4.2 Reissue of multi-domain certificates

The applicants that apply the DQ certificate through other business:

1. The applicant fills out the application information and submits an application through the address that CNNIC URL specified.

2. During the period of validity of the certificate, after the user submits the application, the system will automatically detect whether the information submitted is the correct information. If the information of application consistent with the original message (mostly commissioner's information, company information, etc.), this reissue application will be approved , if the application of certificate is valid for more than one-years, will be rigorous audit conducted at the annual inspection.

3. CNNIC Trusted Network Service Center issues a certificate and the certificate application commissioner installs it.

4.3.5 Renewal and Inspection of DQ Certificates

When a certificate subscriber's certificate expires, the certificate subscriber shall acquire a new certificate to maintain the continuity of the use of the certificate. The certificate subscriber generates a new key pair to replace the expired key pair, which is called "key renewal". However, in some cases, the certificate subscriber hopes to apply for a new certificate for the existing key pair, which is called "certificate renewal".

In the certificate system of CNNIC Trusted Network Service Center, the renewal of a certificate requires the certificate subscriber to generate another certificate request document CSR, and at the same time, CNNIC Trusted Network Service Center requires the certificate subscriber to use a key pair different from the original key pair to apply, and the use of the old certificate request document CSR is not allowed (that is, "key renewal" must be carried out).

The certificate renewal period is within three months before the current certificate becomes invalid. Before or after this period, CNNIC Trusted Network Service Center will reject the application for renewal.

After the renewal, the new certificate shall be immediately installed after being downloaded. The period of validity of the renewal is postponed accordingly, that is

the period before the new certificate becomes invalid = current time + the length of time for the newly purchased certificate + the length of remaining time of the current certificate.

4.3.5.1 Renewal of single domain certificates

The applicants that apply the DQ certificate through other business:1. Users of ".CN" or "中国" domain names registered by CNNIC with real names can log on the URL specified by CNNIC to update the certificate.

2. Applicants for the certificates of CN or "中国" domain names not registered by CNNIC with real names need to submit the following materials to the LRA.

    1> Confirm the e-applications confirmation, including application protocols
    2> Photocopy of the identity of the commissioner shall be submitted.
    3> Photocopy of the enterprise legal person business (affixed with an official seal) or photocopy of the organization code certificate (affixed with an official seal).

1.

3.The LRA entry clerk carries out a preliminary examination. Through whois function, the entry clerk gets the information of the domain name registrant of the domain name certificate application, and checks whether the domain name registrant is consistent with the domain name certificate applicant, and carries out preliminary examination to confirm the domain name certificate applicant indeed holds such domain name.

4. After preliminary examination, the entry clerk at the LRA will upload the above information into RA system, submit the application, and transfer all the paper application materials to the RA auditor at the CNNIC Registration Authority with a safe method. In case of failure of passing the preliminary examination at the LRA, the domain name certificate applicant is required to re-apply after the change of information of the domain name registrant.

5. The RA auditor checks whether the legal domain name holder is consistent with the certificate applicant (also using the whois function), and whether the information is authentic, and compares it with the application information in the RA system.

6.   After the auditor approves the application, the system will send the link for DQ certificate registration to the commissioner; in case of failure of passing the system audit, the application for certificate registration will be rejected, and the user will be informed of the reason.

7.   After logon through the certificate registration link, the system needs to verify the domain name ownership; and the system will send a validation email to the domain name holder, and the user can validate it by clicking the link provided in the email. The certificate will not be downloaded until successful validation, and the certificate will not be issued in case of failure of validation.

4.3.5.2 Renewal of multi-domain certificates

1.   Users of CN or "中国" domain names registered by CNNIC with real names can log on the URL specified by CNNIC to update the certificate.

2.   Applicants for the certificates of CN or "中国" domain names not registered by CNNIC with real names need to submit the following materials to the LRA.

1> Confirm the e-applications confirmation, including application protocols

2> Photocopy of the identity of the commissioner shall be submitted.

3> Photocopy of the enterprise legal person business (affixed with an official seal) or photocopy of the organization code certificate (affixed with an official seal).

3.   The LRA entry clerk carries out a preliminary examination. Through whois function, the entry clerk gets the information of the domain name registrant of the domain name certificate applied for, and checks whether the domain name registrant is consistent with the domain name certificate applicant, and carries out preliminary examination to confirm the domain name certificate applicant indeed holds such domain name.

4.   After preliminary examination, the entry clerk at the LRA will upload the above information into RA system, submit the application, and transfer all the paper application materials to the RA auditor at the CNNIC Registration Authority with a safe method. In case of failure of passing the preliminary examination at the LRA, the domain name certificate applicant is required to re-apply after the change of

information of the domain name registrant.

5. The RA auditor checks whether the legal domain name holder is consistent with the certificate applicant (also using the whois function), and whether the information is authentic, and compares it with the application information in the RA system.

6. After the auditor approves the application, the system will send the link for DQ certificate registration to the commissioner; in case of failure of passing the system audit, the application for certificate registration will be rejected, and the user will be informed of the reason.

7. After logon through the certificate registration link, the system needs to verify the domain name ownership; and the system will send a validation email to the domain name holder, and the user can validate it by clicking the link provided in the email. The certificate will not be downloaded until successful validation, and the certificate will not be issued in case of failure of validation.

4.3.5.3 Types of Certificate on Annual Audit

Annual audit of certificate is to ensure the validity of user information, application period for the extra 1-year certificate will implement the annual inspection system. Auditor will conduct an annual audit of the effectiveness of user information, the inspection process is same as the application process, but without requiring the user to submit the data, but by the CNNIC launched their own trusted network of service centers to the third party inspection.

4.3.6 Revocation of certificates

4.3.6.1 Circumstances for revocation

In any of the following cases, CNNIC Trusted Network Service Center shall be entitled to revoke a domain name certificate that it has issued:

1. Discovering that there is false information in the materials provided by the certificate subscriber to apply for the domain name certificate;

2. The certificate subscriber fails to fulfill the obligations stipulated in the

certificate subscriber's agreement;

3. The certificate subscriber requests the revocation of the domain name certificate;

4. The subject of the certificate subscriber disappears;

5. The certificate subscriber changes the purposes of the domain name certificate;

6. Other circumstances required by laws or regulations.

4.3.6.2 Procedure of revocation

If a circumstance other than the third item of Section 4.3.6.1 arises, CNNIC Trusted Network Service Center will automatically revoke the domain name certificate and notify the certificate subscriber.

The certificate subscriber also has the right to apply for revocation of a certificate and the process of applying for revocation is as follows:

4.3.6.3 Revocation of single domain and multi-domain certificates

The applicants that apply the DQ certificate through other business:

1. The certificate holder submits the electronic application materials for revoking the certificate to the LRA entry clerk.

2. The LRA entry clerk enters the above materials through the RA system and submit the application.

3. The LRA entry clerk transfers all the application materials to the RA auditor at to the RA auditor at the CNNIC Registration Authority with a safe method.

4. The RA auditor checks the materials and compares them with the application information in the RA system and the original registration information of domain name certificate. And confirm it with the person in charge (if any) and the commissioner respectively by telephone.

5. After examination and approval, the RA auditor will revoke the domain name certificate directly. In case of failure of passing the examination, revocation of the certificate will be rejected, and all materials together with the reasons for rejection will be returned to the LRA. After the contact and communication between the LRA

and the commissioner, re-application for revocation can be performed after modification in accordance with the reason of rejection.

6. The system will release a CRL notice about the revocation of the certificate, time of revocation, reason, etc.

4.3.6.4 Revocation of effectiveness

CNNIC Trusted Network Service Center releases the status of revocation on the Certificate Revocation List (CRL), and the effectiveness of a certain certificate will be terminated.

4.3.6.5 Entities that can request the revocation of a certificate

CNNIC Trusted Network Service Center or the certificate subscriber may request the revocation of a certificate under circumstances described in Section 4.3.6.1 of this CPS.

4.3.6.6   Process of request for revocation

When CNNIC Trusted Network Service Center has sufficient reason to believe that a certificate shall be revoked, the related personnel of the Certificate Authority or the Registration Authority of CNNIC Trusted Network Service Center may submit request for revoking the certificate through a process determined internally. After the revocation of the certificate, CNNIC Trusted Network Service Center will notify the certificate subscriber of the revocation of the certificate and the reason for revocation with a proper method, including mail and fax etc.

The certificate subscriber may also request the revocation of its own certificate through the procedure of revocation. When the certificate subscriber submits a request for revocation, it shall also provide the materials provided for application for the certificate as the information for identification.

4.3.6.7 Time limit for putting forward a request for revocation

When any of the cases in Section 4.3.6.1 of this CPS is discovered to arise, the time interval from the discovery of the need to revoke a certificate to putting forward the

request for revocation shall not exceed 24 hours.

4.3.6.8 Time limit for processing a request for revocation by CNNIC Trusted Network Service Center

The time between the receptions of a request for revocation (including paper materials) to the completion of the processing of the request by the Registration Authority (RA) of CNNIC Trusted Network Service Center shall not exceed two (2) working days. The working days of CNNIC Trusted Network Service Center do not include weekends or national holidays.

4.3.6.9 Relying parties' requirement on checking the revocation of a certificate

Whether or not a relying party checks the revocation of a certificate is completely determined by the relying party's requirement on security.

4.3.6.10 CRL release frequency

The certification system of CNNIC Trusted Network Service Center issues one Certificate Revocation List (CRL) of intermediate root every seven (7) days.
CRL issued by root will be renewed every half a year (182 days), if there is no revocation of intermediate root. And CRL of root will be renewed immediately when intermediate root are revoked.

4.3.6.11   Maximum latency for CRL releasing

The latency for a domain certificate from its revocation to its being publicized on the CRL shall not exceed one hundred sixty-eight (168) hours. CRL of the root will be renewed immediately when intermediate root is revoked.

4.3.6.12 Availability of certificates online status inquiry

CNNIC Trusted Network Service Center provides the online inquiry service for certificate status (OCSP). This service is available 7×24 hours every week except at most four (4) hours' regular maintenance and emergency maintenance.

4.3.6.13 Other forms for releasing information on revocation

At present, CNNIC Trusted Network Service Center provides CRL inquiry through the HTTP service.

4.3.6.14   Special requirements on key damage

Whether a certificate subscriber or CNNIC Trusted Network Service Center, once discovering a certificate key suffers from security damage, shall immediately revoke the certificate.

4.4 Certificate freezing

Not applicable. CNNIC Trusted Network Service Center does not support the freezing of certificates.

4.5 Certificate renewing

Not applicable. CNNIC Trusted Network Service Center does not support the renewal of certificates when the key is not replaced.

4.6 Certificate Releasing

The domain name certificates issued by CNNIC Trusted Network Service Center are not released in the repository, but users could check domain name certificates registry information through CNNIC Trusted Network Service Center's website.

4.7 Procedures of computer security auditing

4.7.1 Types of recorded events

All the important security events of CNNIC Trusted Network Service Center are recorded manually or automatically in the protected auditing tracking records. Such

events include but not limited to the following contents:

- ◆ Suspicious network activities

- ◆ Several attempts at entry but unable to access

- ◆ Events relating to installation of equipment or software, modifying and arranging the system of CNNIC Trusted Network Service Center

- ◆ Process of related personnel's access of various parts of CNNIC Trusted Network Service Center

The operations of regular management certificates are also included in the auditing tracking records. These operations include but not limited to the following contents:

- ◆ Deposing request for revocation of certificate

- ◆ Actual issue (including certificate registration, renewal and reissue etc.) and revocation of certificate

- ◆ Updating the information in the repository

- ◆ Compiling the Certificate Revocation List (CRL) and publishing new data

- ◆ Key switch in the Certificate Authority

- ◆ Archive backup

- ◆ Emergency key recovery

4.7.2 Number of times of record processing

CNNIC Trusted Network Service Center processes auditing and tracking records every week to audit and track the related actions, transactions and procedures of CNNIC Trusted Network Service Center.

4.7.3 Retention period of auditing and tracking records

The retention period of auditing and tracking records is ten (10) years.

4.7.4 Protection of auditing and tracking records

CNNIC Trusted Network Service Center practices control by several persons in

processing auditing and tracking records and adequate protection can be provided to prevent the related records from being accidentally damaged or being maliciously changed.

4.7.5 Backup of audit tracking records

CNNIC Trusted Network Service Center makes appropriate backup of audit tracking records every week according to a preset program. Backup can be stored separately away from the computer and have sufficient protection to avoid being stolen, damaged or media disintegration.

4.7.6 Audit tracking records collection system

None

4.7.7 Security events informing

CNNIC Trusted Network Service Center has an automatic monitoring system, which can report important security events to the proper personnel or systems of CNNIC Trusted Network Service Center.

4.7.8 Fragility evaluation

Fragility evaluation is part of the risk evaluation of CNNIC Trusted Network Service Center: according to auditing records, CNNIC Trusted Network Service Center regularly carries out fragility evaluation in terms of technical security and management security and adopts consolidation measures according to the evaluation reports.

4.8 Record archiving

4.8.1 Types of archived records

CNNIC Trusted Network Service Center shall ensure that the archived records include sufficient information so as to determine that whether certificates are valid and whether their past operations are proper. CNNIC Trusted Network Service Center shall keep the following data:

◆ System equipment structure archives

◆ Evaluation results and equipment qualification review records

◆ All versions of the Certificate Practice Statement

◆ Agreements binding upon CNNIC Trusted Network Service Center

◆ All the certificates issued and Certificate Revocation List (CRL)

◆ Regular event records

◆ Other work logs used to verify achieved contents

4.8.2 Retention period of archives

The above archived records shall be properly kept at least over ten (10) years. Auditing and tracking archives shall be kept with a method deemed as proper by CNNIC Trusted Network Service Center.

4.8.3 Archive protection

The archiving media preserved in CNNIC Trusted Network Service Center are protected by various substantive or encrypted measures and can avoid unauthorized access. Protective measures are adopted to protect archiving media from environmental injuries by temperature, humidity and magnetic field.

4.8.4 Archive backup procedure

Making and preserving archived copies.

4.8.5 Timestamp

Archived materials shall be marked with the starting time and date of the archived items. CNNIC Trusted Network Service Center uses control measures to prevent unauthorized adjustment of the system clock.

4.9 Change of key

The life of the Certificate Authority root keys of the certificates generated by the Certificate Authority of CNNIC Trusted Network Service Center to prove the certificates issued according to this CPS and the life of the certificates do not exceed twenty (20) years. The Certificate Authority keys and certificates of CNNIC Trusted Network Service Center are renewed at least three months before the term expires. After being renewed with a new root key, the related root certificates will also be publicized for the use of the public. The original root keys will be kept to the shortest term designated in Section 4.10.2 for the check of certificates signed with the original root keys.

4.10 Termination of services of CNNIC Trusted Network Service Center

When the services of CNNIC Trusted Network Service Center are terminated, CNNIC Trusted Network Service Center will revoke all the certificates issued by CNNIC Trusted Network Service Center, and will transfer the archived records of CNNIC Trusted Network Service Center to an agency stipulated by laws and regulations.

After the termination of services, CNNIC Trusted Network Service Center will save the records of its Certificate Authority for ten (10) years (calculated from the date

when services are terminated); these records include root certificates and intermediate root certificates, issued domain name certificates, Certificate Practice Statement and Certificate Revocation List (CRL).

4.11 Disaster recovery and key compromise plan

4.11.1 Disaster recovery plan

CNNIC Trusted Network Service Center has prepared a proper business continuity plan, including daily backup of primary business information and system data of the Certificate Authority, and proper backup of system software of the Certificate Authority to maintain the continuous operation of its primary business, and to guarantee that it can continue to provide services or restore services within the shortest time under the influence of serious breakdown or disaster.

Every year, the business continuity plan will be reviewed and carried out strictly.

CNNIC Trusted Network Service Center has a disaster recovery base outside its production base. In case of a serious breakdown or disaster, CNNIC Trusted Network Service Center will notify the government department in time and announce that its operations will be transferred from the production base to the disaster recovery base.

After the occurrence of a disaster but before the re-establishment of a stable and reliable environment:

◆ Sensitive materials or instruments will be safely locked within the facilities;

◆ If sensitive materials or instruments cannot be safely locked within the facilities or these materials or instruments are subject to risks of being damaged, these materials or instruments will be moved away from the facilities and locked within other temporary facilities;

◆ Access control will be practiced for the entry and exit of facilities to avoid being stolen or being accessed without authorization.

4.11.2 Key compromise coping plan

The business continuity plan includes the coping plan for dealing with key compromise. These plans will be reviewed every year.

If the private key information of the root certificates or intermediate root certificates of CNNIC Trusted Network Service Center used to issue domain name certificates according to this CPS is disclosed, CNNIC Trusted Network Service Center will publicize it in time. Once the private key information of the root certificates or the intermediate root certificates of CNNIC Trusted Network Service Center is disclosed, CNNIC Trusted Network Service Center will revoke in time the certificates issued with the private key and then issue new certificates to replace them.

4.11.3 The transfer of the key

In case of key information compromise or disaster, the private key information used by CNNIC Trusted Network Service Center to issue domain name certificates according to this CPS is disclosed or damaged and cannot be recovered, CNNIC Trusted Network Service Center will publicize it. Publicized contents include the list of certificates that have been revoked, how to provide certificates subscribers with new public key of the root certificates or intermediate root certificates of CNNIC Trusted Network Service Center and how to reissue certificates to certificate subscribers.

4.12 Emergency process of CNNIC Trust Network Service Centor.

CNNIC Trust Network Service Centor provide emergency process for 24*7. please contact CNNIC at 010-58813000 to handle emergency case.

5 Operation specification of Subordinate CA authorization

5.1 Management process of subordinate CA authorization

CNNIC will issue subordinate CA certificate as following procedures,
1. The applicant apply for being subordinate CA of CNNIC.
2. The qualification of applicant will be reviewed by CNNIC Trust Network Service Center, see 5.2 for more details.
3. CNNIC Trust Network Service Center will give evaluation to the application through review and risk assessment.
4. The Security Management Committee of CNNIC will make decisions according to the evaluation mentioned in 5.1.3.
5. Once the cooperation is determinated, CNNIC will sign the agreement with the applicant.
6. CNNIC will disclose the structure and purpose of the subordinate CA certificate in CP and CPS, in the meanwhile, CNNIC will disclose information to Browsers and Operation System manufacturer (Microsoft, Apple, Google, and Mozilla).
7. CNNIC will start the issuance process of subordinate CA certificate, see 5.3 for more deatails.
8. CNNIC will disclose the subordinate CA certificate to the public.

CNNIC will verify the subordinate CA audit report according the audit cycle after the subordinate CA certificate is issued and published.

5.2 Qualificiation Review

1，The applicant provide application letter sealed and signed, essential information of the applicant (Sealed copy of Business license, etc.), CP and CPS which is published in the applicant's official website, WebTrust audit report. The subordinate CA's policy and procedure documents, include but not limited to: Design document and management policy of machine room, Hardware security module and private key management policy.
2，Generation of key pairs and verification
CNNIC will assign a person to verify key pairs generation of subordinate CA, the working process is including:
A. Pre-study on design document and management policy of machine room, Hardware security module and private key management policy, as well as the articles in CP/CPS about environment, access control, hardware

security module management, and private key management.

    B.   Participate and witness the suboridinate CA's key pairs generation ceremony, verify the following contents,

- prepare a Key Generation Script,
- Key generation script should comply CPS/CP and meet the requirement of key pairs management.
- Follow the key generation script.
- generate the keys in a physically secured environment as described in the CA's CP/CPS
- generated the keys in a Hardware security modul as described in the CA's CP/CPS.
- Generate the key pairs using personnel in trusted roles under the principles of multiple person control, comply to CA's CP/CPS, Hardware security module management policy.
- Check the Hardware security moule logs to ensure the Key generation activities is record successfully.

3. WebTrust audit report verification.

CNNIC will assign a person accountable for verifying the subordinate CA's WebTrust audit report regularly, including:

A. Determine the validity of the the subordinate CA's WebTrust audit report in WebTrust official website.

B. Communicate with auditors about the key point which should be in the report in advance, and confirm them in Subordinate CA's report.

C. If there is any findings in subordinate CA's audit report, CNNIC will initiate risk assessment process to determine whether CNNIC should revoke the suboridinate CA certificate or take other steps, and disclose all the information to the public.

4. Risk assessment

CNNIC will collect and summarize documents including but not limit to 1,2,3 above. After preparing, CNNIC will reach to a risk assessment report through meeting discussion.

5.3 Subordinate certificate issuance and record.

CNNIC will issue the subordinate CA certificate according to the review result in 《Subordinate certificate issuance and record form》 (Appendix B in CP). Fully recording the certificate issuance process and publicly disclose the certificate.

5.4 Revoke Subordinate certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing；

2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Appendix A,
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with these Baseline Requirements or the applicable Certificate Policy or Certification
Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

6 Control of Physical, Program and Personnel Security

6.1 Physical security

6.1.1 Site selection and construction

The operations of CNNIC Trusted Network Service Center are at a location with

reasonably safe conditions. In the course of site construction, CNNIC Trusted Network Service Center has adopted appropriate preventive measures to make preparation for the operations of CNNIC Trusted Network Service Center.

6.1.2 Access control

CNNIC Trusted Network Service Center implements reasonable security control to limit the access to the hardware and software (including servers, work stations and any external encrypted hardware modules) used in CNNIC Trusted Network Service Center. Personnel who can access the above hardware and software are limited to the personnel that perform trusted responsibilities described in Section 5.2.1 of this CPS. At any time, the above access is controlled and monitored electronically to prevent unauthorized inbreak.

6.1.3 Electric power and air-conditioning

The electric power and air-conditioning resources that can be acquired at CNNIC Trusted Network Service Center include dedicated air-conditioning system, uninterrupted power supply system (UPS) and mobile generating set rented from an electric power company to supply electric power in case of breakdown of the urban electric power system.

6.1.4 Natural disasters

The facilities at CNNIC Trusted Network Service Center can be free from impact of natural disasters within a reasonably possible limit.

6.1.5 Fire control and protection

CNNIC Trusted Network Service Center has prepared an appropriate fire control plan and fire fighting system for its facilities.

6.1.6 Media storage

Media storage and disposal procedures have been well prepared.

6.1.7 Off-site backup

Proper backup system data of CNNIC Trusted Network Service Center will be stored off site and have adequate protection to avoid being stolen, damaged or media disintegration.

6.1.8 Printed documents keeping

Printed documents (including the identity confirmation documents of the certificate subscribers and management files etc.) are properly kept at CNNIC Trusted Network Service Center, which can only be retrieved by authorized personnel.

6.1.9 Waste material disposal

Waste materials are disposed according to normal waste disposal requirements. Before discard of encrypted equipment, physical damage or reset shall be carried out according to the guidance of the equipment manufacturer.

6.2 Process control

6.2.1 Trusted responsibilities

The personnel at CNNIC Trusted Network Service Center who can access critical areas, control passwords or other operating programs and may exert major influence on the issue, use and revocation of certificates shall be deemed as bearing trusted responsibilities. Such personnel include but not limited to system management personnel, operators, engineering personnel and administrative personnel appointed to supervise the operations of CNNIC Trusted Network Service Center.

CNNIC Trusted Network Service Center has developed related management systems for all the personnel who assume trusted responsibilities for being involved in the domain name certificate services of CNNIC Trusted Network Service Center, including:

˙Developing various levels of physical and system operation control processes according to roles and responsibility

˙Detailed regulations on responsibility division

6.2.2 Document and material transfer between CNNIC Trusted Network Service Center and Local Registration Authority (LRA)

The transfer of all the documents and materials between CNNIC Trusted Network Service Center as well as the Registration Authority (RA) belonging to it and Local Registration Authority (LRA) is carried out with a controlled and safe method.

6.2.3 Annual evaluation

An annual evaluation is carried every year at CNNIC Trusted Network Service Center to ensure that daily operation processes meet security policies and other related regulations on process control.

6.3 Personnel control

6.3.1 Backgrounds and qualifications

The backgrounds, qualifications and record of service of the working personnel of CNNIC Trusted Network Service Center shall be verified and examined. They shall be sincere and reliable, have enthusiasm for work, not take part-time job affecting system operation, not have major error record in the same trade or law-breaking records etc.

Background: high political competence, excellent professional competence, very strong sense of responsibility, being highly-principled, without criminal record and bad record;

Qualifications and record of service: expert at the job of the post; the education and training received as well as working experience guarantee that they are adequate for their job;

The working personnel of CNNIC Trusted Network Service Center and its management policies can reasonably ensure the reliability and competence of CNNIC Trusted Network Service Center or represent the reliability and competence of the LRA personnel of CNNIC Trusted Network Service Center and can ensure that they perform their responsibilities according to this CPS.

6.3.2 Background investigation

CNNIC Trusted Network Service Center (including the Registration Authority) carry out investigation on the personnel that take up trusted responsibilities (carried out before recruitment and when necessary after recruitment), to verify the reliability and competence of the working personnel according to this CPS and the personnel policy of CNNIC Trusted Network Service Center. Personnel failing to pass the first investigation or regular investigation cannot take up or continue to take up trusted responsibilities.

6.3.3 Requirements on training

The working personnel of CNNIC Trusted Network Service Center (including the Registration Authority) have accepted the preliminary training required for performing their responsibilities. CNNIC Trusted Network Service Center will provide continuous training so that its personnel can grasp the required latest working skills.

6.3.4 Documents provided to personnel

The personnel at CNNIC Trusted Network Service Center (including the Registration Authority) will receive a guidance manual, which details the registration, renewal, reissue and revocation procedures of certificates as well as other software functions related to their responsibilities.

7 Technical safety control

7.1 Generation and installation of keys

7.1.1 Generation of key pairs

Root CA: the key pair of root CA is directly generated by hardware encryption equipment and is directly saved in the hardware encryption equipment (encryptor). CNNIC Trusted Network Service Center uses the encrypted hardware equipment that has passed the appraisal of the State Commercial Code Management Commission. A key must be generated by encrypted hardware equipment after three of five key administrators log on simultaneously, and any single administrator cannot carry out operations for generating a key. Key administrators log on by adopting IC card method, and other personnel cannot acquire an IC card or corresponding password.

Operation CA: the key pair of operation CA is generated on local hardware encryption equipment (hardware encryption equipment used is encrypted hardware equipment that has passed the appraisal of the State Commercial Code Management Commission), and private keys cannot be away from this encrypted hardware equipment. A key must be generated by encrypted hardware equipment after three of five key administrators log on simultaneously, and any single administrator cannot carry out operations for generating a key. Key administrators log on by adopting IC card method, and other personnel cannot acquire an IC card or corresponding password.

Certificate applicant: a signature key pair is generated at the terminal of the certificate applicant, with strict and secure control measures. CA servers cannot provide certificate applicants with services for key generation. CNNIC Trusted Network Service Center does not provide key media for certificate applicants.

7.1.2 Transfer of public key to certificate issuer

A certificate applicant shall use the Web server software to encapsulate the public key into a certificate request in the PKCS #10 format and send it to CNNIC Trusted Network Service Center, where a certificate is generated.

CNNIC Trusted Network Service Center will verify the completeness of the certificate request according to the certificate request submitted by the certificate applicant, and CNNIC Trusted Network Service Center only processes complete certificate requests.

7.1.3 CNNIC Trusted Network Service Center's public key releasing

CNNIC Trusted Network Service Center will release its public key on the website to be retrieved by the final entities.

7.1.4 Key sizes

The key pair of root certificates and intermediate root certificates of CNNIC Trusted Network Service Center is 2,048 digits RSA. The key pair of a certificate applicant is also 2,048 digits RSA.

7.1.5 Password module standard

Generation of signature keys, storage and signature operations are carried out in hardware password modules. Hardware password modules are safe products that have passed the examination of the state authority in charge of passwords in China and

meet the related state regulations.

7.1.6 Keys purposes

The keys used for the domain name certificates of CNNIC Trusted Network Service Center can be used in encrypted communication. The keys of root certificates and intermediate root certificates of CNNIC Trusted Network Service Center are only used in issuing certificates and Certificate Revocation List (CRL).

7.1.7 Destruction of keys

The keys of root certificates and intermediate root certificates of CNNIC Trusted Network Service Center shall be archived and retained for ten (10) years after they become invalid and then be destroyed with an appropriate method. After the archiving term of the archived keys expires, they shall be safely destroyed with the participation of several trusted staff members. The destruction of keys shall ensure that their private keys be thoroughly deleted from the hardware password modules, without retaining any residual information.

The private key of a certificate applicant exists at the terminal of the certificate applicant and shall be immediately destroyed after the certificate expires.

7.2 Private key protection and password module project control

7.2.1 Standard of password modules

The hardware password modules adopted by CNNIC Trusted Network Service Center are safe products that have passed the examination of the state authority in charge of passwords in China and meet the related state regulations. Hardware password modules are installed in safe areas and the keys stored in an encrypter can be accessed when at least three encrypter administrators (key administrators) are present.

When an encrypter is being backed up and restored, there must be three administrator password cards simultaneously in order to carry out backup and restoration of the encrypter.

7.2.2 Private keys controlled by muti-person

The keys stored in an encrypter can be accessed only when the majority of the administrators are at present at the same time. Protective measures that have passed the examination of the state authority in charge of passwords in China are adopted to guarantee the security of the keys inside the encrypter.

Specifically, CNNIC Trusted Network Service Center adopts the policy of control by five persons and simultaneous presence of three persons for the protection of the keys of root certificates and intermediate root certificates.

7.2.3 Private key custody

The private keys of the root certificates and intermediate root certificates of CNNIC Trusted Network Service Center are not entrusted to another agency, nor does CNNIC Trusted Network Service Center accept the entrustment from any certificate applicant to keep signature private keys.

7.2.4 Backup of private keys at CNNIC Trusted Network Service Center

As a measure for disaster recovery, key backup shall be carried out. CNNIC Trusted Network Service Center adopts hardware password modules meeting state regulations to encrypt and back up root certificates and intermediate root certificates, and the backup is stored within a system independent from the hardware password module system. When backing up keys, the key administrator must use a password IC card to start the key management program and execute the key backup order in order to complete the backup.

The private key of a certificate applicant is stored at the terminal of the certificate applicant. The certificate applicant shall store, back up and restore its private key according to specific conditions and by adopting an appropriate measure.

7.3 Other aspects of key pair management

7.3.1 Public key archiving

The administrator operates the archiving of the certificates and public keys of CNNIC Trusted Network Service Center.

7.3.2 Private key archiving

After the key pairs of root certificates and intermediate root certificates expire, these key pairs will be archived and retained for at least ten (10) years. The archived key pairs are saved in the hardware password modules described in Section 6.2.1, and the CNNIC key management policy and process prevent archived key pairs from returning to the production system. After the archiving retention period of the archived key pairs expires, CNNIC Trusted Network Service Center will destroy them according to the provisions in Section 6.1.7 of the CPS.

The private keys of certificate applicants are kept at the terminal of certificate applicants; therefore, archiving does not apply to the private keys of certificate applicants.

7.3.3 Certificate operation period and key pair usage period

The usage period of the public keys and private keys of the root certificates and intermediate root certificates of CNNIC Trusted Network Service Center are consistent, with the usage period of key pairs of root certificates being twenty (20) years and the usage period of key pairs of intermediate root certificates being ten (10) years.

The longest usage period of the domain name certificates of CNNIC Trusted Network Service Center is three(3) years. Certificates can be renewed within a period before the date of expiry.

7.4 Computer security control

CNNIC Trusted Network Service Center operates under a safe environment and practices subarea access authority control. The core system is insulated from other systems, with firewall and invasion inspection to ensure its safety. Also, the following are carried out:

Systems are safely configured and unnecessary services and ports are closed.

The operating system must be installed with the latest program patches and a person is specially assigned to be responsible for the installation of the latest patches.

A person is specially assigned to be responsible for each machine in the production system, computer operation procedure shall be strictly followed, and password is managed level by level and authorized level by level. Each person is responsible for the operation of their own scope of authority.

Auditing system of logs and operating records.

Data backup and recovery mechanism

7.5 Life cycle technical safety control

The certificate life cycle safety control follows the WebTrust certification code.

The systems used at CNNIC Trusted Network Service Center have all gone through detailed test before use and irregular examination is carried out in the course of use.

7.6 Network security control

According to different requirements on security, the systems at CNNIC Trusted Network Service Center are divided into different network sections and some systems at high security level carry out offline operations. Also, a hierarchy model is adopted

to ensure network security and system reliability.

7.7 Password module engineering control

The password modules used at CNNIC Trusted Network Service Center are encypters that have passed the examination of the state authority in charge of passwords in China.

8 Structure of Certificates and Certificate Revocation List (CRL)

8.1 Structure of certificates

The certificates mentioned in this CPS include public keys used to confirm identity and verify whether the information is complete. The certificates mentioned in this CPS are all issued in the format of the third version of X.509.

8.1.1 Version number

The domain name certificates of CNNIC Trusted Network Service Center have extensive universality. The certificate format meets the X.509 V3 standard and can provide the ability to support certificate extension.

8.1.2 Certificate items description

Suboridinate CA certificate structure

Domain	Value or distriction of value
Basic	
Version	V3
Serial Number	Unique value of the certificate issued by TNS Center of CNNIC
Signature Algorithm	sha256RSA

Hash	sha256
Issuer	CN = CNNIC ROOT O = CNNIC C = CN
Valid from	Represent certificate effective time. Universal Coordinate Time base. Synchronized to Master Clock of China.
Valid to	Represent certificate end time. Universal Coordinate Time base. Synchronized to Master Clock of China.
Subject	The distinguished name of certificate subscriber.
Public Key	Certificate public key. Use RSA algorithm. The length of key is 2048 bit.
extensions	
Basic Constraint	Subject Type=CA Path Length Constraint=None（Set value(0,1,2,3) As actual sistuaction)）

CRL Distribution Point	CRL Distribution Point
	    Distribution Point Name:
	       Full Name:
	          URL=http://crl.cnnic.cn/download/rootsha2crl/CRL1.crl

Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
SubjectKeyIdentifier	Indentifier of a Subordinated CA certificate public key
AuthorityKeyIdentifier	KeyID=65 f2 31 ad 2a f7 f7 dd 52 96 0a c7 02 c1 0e ef a6 d5 3b 11

Certificate Policy	[1]Certificate Policy:
	    Policy Identifier=1.3.6.1.4.1.29836.1.6
	    [1,1]Policy Qualifier Info:
	      Policy Qualifier Id=CPS
	      Qualifier:
	        http://www.cnnic.cn/cps/

Authority Info Access	[1]Authority Info Access
	    Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
	    Alternative Name:
	        URL=http://ocspcnnicroot.cnnic.cn
	[2]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:

	URL=http://www.cnnic.cn/download/cert/CNNICROOT.cer
Thrumprint Algorithm	Sha1
Thumprint	Certificate Thumprint

Entity certificate structure

Domain	Value or distriction of value
Basic domain	
Version	V3
Serial No.	Unique value of the certificate issued by TNS Center of CNNIC
Signature Algorithm	The algorithm of issuing certificate. See CPS8.1.3 Chapter
Issuer	Name of certificate issuer. The subject name of Domain Name Certificate issuer is TNS Center of CNNIC.
Valid From	Represent certificate effective time. Universal Coordinate Time base. Synchronized to Master Clock of China.
Valid to	Represent certificate end time. Universal Coordinate Time base. Synchronized to Master Clock of China.
Subject	The distinguished name of certificate subscriber.
Public Key	Certificate public key. Use RSA algorithm. The length of key satisfies the requirements in CPS 7.1.4.
Extended	
Basic Restriction	Value of domain certificate is: Subject Type=End Entiry Path Length Constraint=None
CRL Distribution	Certificate issued by TNS Center of CNNIC includes CRL distribution extended attributes. Dependers can download CRL accordint to the address and agreement of this extended attribute.
Key Usage	Value of domain certificate is KeyEncipherment, DigitalSignature

SubjectKeyIdentifier	Indentifier of a domain certificate public key issued
AuthorityKeyIdentifier	Indentifier of higher level's CA certificate public key

Certificate Policy	[1]Certificate Policy:
	    Policy Identifier=1.3.6.1.4.1.29836.1.1
	    [1,1]Policy Qualifier Info:
	        Policy Qualifier Id=CPS
	        Qualifier:
	
	           http://www.cnnic.cn/cps/

Strenghen Key Usage	Value of domain certificate is server authentication
Subject Alternative Names	Value of multi-domain certificate is all domains authenticated by the certificates.

8.1.3 Algorithm object identifier

Algorithm

The algorithm of Certificate issued by CNNIC is sha1RSA and SHA256.

8.1.4 Forms of names

The distinguished names of the certificates issued by CNNIC Trusted Network Service Center meet the regulations of X500 on distinguished names. For certificate subject distinguished names, C represents country, and value is CN; O represents organization, and value is CNNIC or CNNIC SSL or certificates holders' name; CN is many domain names side by side for multi-domain certificates, and single domain name for single domain certificates and wildcard domain certificates.

8.1.5 Limits on names

In DN, all ASCII characters can be used except dedicated characters and special characters. Dedicated characters "\" and """" cannot be used in DN as they have special meaning in DN. Besides, if cn has special characters (",", "=", "+", "#", "<",

">" and ";"), the CA system of CNNIC Trusted Network Service Center will carry out special treatment, that is, to add double quotations marks to the whole cn contents. This will lead to inconvenience in the subsequent actual treatment. Therefore, these special characters are not allowed in cn.

As there are invisible ASCII characters, which are not convenient for certificate applicants to use. The following is the list of all available ASCII characters in this CPS (ASCII value is decimal value):

ASCII value	Character
032	Space
033	!
036	$
038	&
040	(
041	)
045	-
046	.
047	/
048~057	0~9
058	:
065~090	A~Z
091	[
093	]
094	^
095	—
096	`
097~122	A~z
123	{
125	}
126	~

8.1.6 Certificate policies object identifiers

Certificate policies are formulated by the certificate issuing agency and widely publicized externally, and at the same time, standard object identifiers are applied with an the International Standardization Organization so as to ensure that they are compatible with other applications. Object identifiers are passed in communications service, and as the identifiers of the certificate policies of the certificate agency,

represent the related policies of the certificate agency for providing certificate services. On the other hand, only when a certificate applicant agrees with the certificate policies can it apply with the Certificate Authority and acquire a digital certificate.

8.1.7 Usage of policy restriction extensions

It is stipulated that various levels of CA in the CA system use the same CP and whether they trust each other with other CA systems. The domain certificates of CNNIC Trusted Network Service Center do not use the extension field.

8.1.8 Grammar and semantics of policy qualifiers

For this extension field, X.509V3 standard has no prescribed format. The location explanation of CPS online may be provided. The domain certificates of CNNIC Trusted Network Service Center do not use the extension field.

8.1.9 Rules for treating critical certificate policy extensions

The domain certificates of CNNIC Trusted Network Service Center do not use it.

8.2 Structure of Certificate Revocation List (CRL)

The format of the Certificate Revocation List (CRL) of CNNIC Trusted Network Service Center is X. 509 Version II.

8.2.1 Version number

V2

8.2.2 CRL and CRL entry extensions

CRL   Data definition
Version (Version)

Meaning: indicating the version number of CRL.

Signature (Signature).

Meaning: CA signature for issuing CRL.

Algorithm identifier (algorithmIdentifier).

Meaning: defining the algorithm used for issuing CRL.

Issuer of CRL (Issuer)

Meaning: the distinguished name of CA issuing CRL.

CRL release time (thisUpdate)

Estimated update time of the next CRL (next update)

Contents of information about revoked certificates (revoked certificates)

CRL Extension (CRL Extension)

CA's public key identifier (AuthorityKeyIdentifier)

CRL number (CRL Number)

8.3 OCSP

OSCP issued by CNNIC Trusted Network Service Center CA responds to RFC2560 standard. OCSP response shall at least include the following basic fields and contents stated in the following table.

Basic fields of OCSP structure

Field	*Value or value restriction*
Status	Status of response, including success, request format error, internal error, re-try after a while, not signature in request and no authorization in the request signature certificate. When the status is success, the following items must be all included
Version	V1
Signature algorithm	Algorithm for issuing OCSP. Use sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) algorithm in signature.
Issuer	The entity issuing OCSP. The SHAI data abstract value and

	certificate distinguished name of the issuer's public key.
Time of generation	Time of generation of OCSP response.
Certificate status list	Include the certificate status list inquired in the request. The status of each certificate includes certificate identifier, certificate status and certificate revocation information.
Certificate identifier	Include data abstract algorithm (SHA1, OID: 1.3.14.3.2.26), certificate distinguished name data abstract value, certificate public key data abstract value and certificate serial number.
Certificate status	Latest status of a certificate, including valid, revoked and unknown.
Certificate revocation information	When the status of the returned certificate is revoked, the time of and cause for revocation are included.

8.3.1 Version number

V1

8.3.2 OCSP extensions

Consistent with RFC2560

8.3.3 OCSP request

OCSP request at least includes:

Agreement version

Service request

Object certificate identifier

Extensions needed by OCSP server

8.3.4 OCSP response

Correct OCSP response shall include:

Version of response agreement

Name of OCSP server

Response to each certificate of a request (including object certificate identifier, certificate status value, time interval of effective response, alternative extensions)

Alternative extensions

Signature algorithm OID

Signature calculated with hashing function

9 CPS management

9.1 Process of making changes

Before any change is made in the CPS of CNNIC Trusted Network Service Center, CNNIC Trusted Network Service Center will study the terms to be changed and decides to change. After soliciting legal opinions from the lawyers of CNNIC Trusted Network Service Center, the security management committee will form a decision.

After a decision is formed at CNNIC Trusted Network Service Center, the changed CPS of CNNIC Trusted Network Service Center will be publicized at the website of CNNIC Trusted Network Service Center.

CNNIC Trusted Network Service Center will carry out strict version control over its CPS.

9.2 Announcements and notices

All the announcements and notices are publicized at the website of CNNIC Trusted Network Service Center ((http://tns.cnnic.cn).

9.3 CPS approval procedure

The approval process is:

(1) CPS compiling group compiles or revises the CPS.

(2) After being compiled or revised, the CPS is submitted to various departments of CNNIC Trusted Network Service Center for deliberation.

(3) The CPS that has passed the deliberation is submitted to the Security Management Committee of CNNIC Trusted Network Service Center for deliberation.

(4) After the CPS passes the deliberation of the Security Management Committee of CNNIC Trusted Network Service Center, the CPS is formally released externally.

9.4 Interpretation

CNNIC Trusted Network Service Center has the sole right to the interpretation of this CPS.