China Internet Network Information Center (CNNIC)

Trusted Network Service Center

EV Certificate Practice Statement

Version No.: 2.03

Validity from: July 1st, 2013

China Internet Network Information Center (CNNIC)

July 1st, 2013

Control table for versions of EV Certificate Practice Statement of CNNIC Trusted Network Service Center

Version No.	Description on major modifications	Date of completion
V1.00	Passing primary verification	August 31, 2010
V2.00	“Security Management Committee holds four meetings or performs joint signing of documents according to demands each year. “ is changed to “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 “	August 31, 2011
V2.01	Extended the expiration of EV CPS to one year with annual audit	April 7th, 2012
V2.02	1. Modified application materials which not differentiate independent server and hosted server. 2. Add applicant representative in role of applicant. 3. Add electromagnetic protection	
V2.03	1. In terms of verifying the identity and legal character of private organization or business entity, its parent, subsidiaries, or affiliates should also be concerned about. 2. Precautions contents contrapose high-risk applicants (eg financial) should be included.	June 24th, 2013

Table of Contents

Terms and Terminology

CA: Certification Authority

CP: Certificate Policy

CPS: Certification Practice Statement

CRL: Certificate Revocation List

CSR: Certificate Signing Request

EV Certificate: Extended Validation Certificate

HTTP: Hypertext Transfer Protocol

ITU: International Telecommunications Union

PKI: Public Key Infrastructure

PKIX: Public Key Infrastructure X.509

RA: Registration Authority

SSL: Secure Sockets Layer

URL: Uniform Resource Locator

1. General

Trusted Network Service Center, China Internet Network Information Center (hereinafter referred to as “CNNIC”) (hereinafter referred to as “CNNIC Trusted Network Service Center”) complies EV Certificate Practice Statement (hereinafter referred to as “EV CPS”) as the relevant practice and system operation specification of EV Certificate of CNNIC Trusted Network Service Center according to *EV guideline* provided in CA/Browser forum, with a view to organize agencies, governments and enterprises in the provision of domain name intensified trusted server certificate security services (also called “EV Certificate” services) under such Practice Statement. This document provides CNNIC employees, who provide certificate services, with principle and practice statement in law, commerce and technology, including but not limited to approval, issuance, utilization and management of EV Certificate, and bases on X.509 Certificate generated by PKI system in CNNIC Certificate Policy (CP).

1.1 CNNIC Trusted Network Service Center

CNNIC Trusted Network Service Center fulfills the responsibility as certification authority of EV Certificate and carries on its obligations under this EV CPS. It is the only certification authority to issue EV Certificate with the authorization of this EV CPS. As a certificate issuance authority, CNNIC Trusted Network Service Center operates in accordance with PKI system, including request receiving, issuance, revocation and update of a digital certificate as well as maintenance and issuance of Certificate Revocation List (CRL). It conforms to international standards, including *EV guideline* provided by CA/Browser Forum, and other relevant laws and regulations in the whole PKI services.

CNNIC Trusted Network Service Center shows to the replying party that conforms to Section 5.6 and other relevant provisions of this EV CPS that, it issues EV Certificate to a certificate holder in accordance with this EV CPS. The EV certificate issued by CNNIC Trusted Network Service Center will immediately become valid after it has been sent and accepted by the certificate holder.

1.2 Role and responsibility

1.2.1 Security Management Committee

CNNIC Trusted Network Service Center Security Management Committee is responsible for the formulation of security policy, specification and policy. It is also a policy-making authority for security management of CNNIC Trusted Network Service Center. Its responsibility includes: collecting issues and proposal concerning security management and arriving at a consensus; formulation and maintenance of EV Certificate Policy (EV CP) of CNNIC Trusted Network Service Center; and verification on EV Certificate Policy Statement (EV CPS).

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 announce 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 Manager

The Chief Security Manager will take a full charge of daily security affairs in CNNIC Trusted Network Service Center. Authorized by CNNIC Trusted Network Service Center, the Chief Security Manager may execute and alter the security policy of CNNIC Trusted Network Service Center and make a regular examination and evaluation on security management of the Center so to keep the security management at an advanced level and with higher security and credibility. It also keeps track of the latest trend about security management in order to ensure the advance of security system. In order to ensure the safe and reliable management of CNNIC Trusted Network Service Center, the Chief Security Manager of the Center mainly concentrates on the following three key areas: development of security policy;

assistance of program development and execution; maintenance of security policy and program for maturity; correspondence of audit security policy and the actual execution situations.

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

- Set up and alter security policy and specification of CNNIC Trusted Network Service Center after obtaining authorization;
- Manage cross certification; issue cross certification agreement of CNNIC Trusted Network Service Center, update and cancel cross certification and deal with audit report.

1.2.3 Registration Authority (RA)

There is only one registration authority in CNNIC Trusted Network Service Center, located in CNNIC. RA will be responsible for the accepting of EV Certificate application and approval of the certificate applicant and store the EV Certificate application information in the Certification Authority.

1.4 Local Registration Authority (LRA)

CNNIC Trusted Network Service Center delegates the responsibilities of all work in the fulfillment of this EV CPS and Certificate Holder Agreement to Local Registration Authority (LRA). The relevant responsibilities are executed by LRA. CNNIC Trusted Network Service Center will be responsible for the fulfillment of this EV CPS and Certificate Holder Agreement.

The LRA in this Policy Statement refers to the trusted EV server certificate registrar that is certified by CNNIC.

CNNIC Trusted Network Service Center identifies LRA and authorizes it to carry out material collection on the certificate applicant registration. When the certificate applicant makes certificate registration, reissuing, renewal, termination, obtaining of two codes and correction of multiple domain names, LRA shall have the obligation for the collection of

relevant information and primary verification on the accuracy of such information.

1.5 Certificate Applicant

The EV Certificate applicants of CNNIC Trusted Network Service Center include commercial, non-commercial, government and private agencies and are enterprises, organizational institutions and other units according to the national situations of China. The certificate applicant owns private key and its identity information will be shown in the EV Certificate. The EV Certificate applicant firstly needs to make an application for certificate services to CNNIC Trusted Network Service Center. EV Certificate will be issued to it after its identity is verified.

See Section 5.3 below for the duties and obligations of certificate holders.

1.6 Certificate holder and relying party

According to this EV Certificate Policy Statement, there includes two types of entities, EV Certificate holder and the relying party.

The certificate holder may be certificate holding agency, which is the holding and using party of EV Certificate. The certificate holder may not transfer any right conferred under Certificate Holding Agreement or Certificate and any transfer shall be seen as invalid.

The relying party trusts the trusted EV server certificate issued by CNNIC Trusted Network Service Center. We hereby make clear that what the relying party trusts is not certificate registrars like Trusted Network Service Registration Authority (hereinafter referred to as “Registration Authority” or “RA”) or Local Registration Authority (LRA) but CNNIC Trusted Network Service Center. CNNIC Trusted Network Service Center issues digital certificate through RA and RA has no occupational responsibility for the relying party and carries on no responsibility towards the relying party on the issuance of digital certificate.

1.7 EV CPS of CNNIC Trusted Network Service Center

The Extended Validation Certificate Practice Statement of CNNIC Trusted Network Service Center is an open practice standard. CNNIC Trusted Network Service Center issues,

revokes and updates EV Certificate under its certificate chain. This EV Certificate Practice Statement mainly includes the following parts: technology, structural architecture, practice and law.

The certificate policy issuing authority of CNNIC Trusted Network Service Center is responsible for maintaining such EV Certificate Practice Statement, relevant agreements as well as relevant certificate policies in this document. The contact means of certificate policy issuing authority of CNNIC Trusted Network Service Center is:

Trusted Network Service Center, China Internet Network Information Center

Add: 4, South 4th Street, Zhongguancun, Haidian district,, Beijing 100190

Tel: 58813075

For this EV Certificate Practice Statement, Certificate Policy and relevant specifications, please refer to CNNIC Website (http://www.cnnic.cn/index/0T/index.htm).

1.8 Applicability, correction and publishing of EV CPS

The certificate policy issuing authority of CNNIC Trusted Network Service Center is responsible for describing the applicability of Certificate Policy in this EV Certificate Practice Statement. Meanwhile, it will carry on responsibility for the applicability of modified parts of EV Certificate Practice Statement before the next version is issued.

When the certificate policy issuing authority thinks that the altered parts of EV Certificate Practice Statement make a heavy influence on certificate users, the updated version shall be issued on the website within seven days and the altered Version No. and altered parts shall be explained in detail.

If certificate policy issuing authority thinks that the altered parts of EV Certificate Practice Statement makes a little or little influence on certificate users, there is no need to inform users and correct the Version No. of altered EV Certificate Policy Statement.

Before CNNIC Trusted Network Service Center makes any alternation on EV CPS, it will make research on clauses to be altered and then make the decision for alternation. After consulting the attorney of CNNIC Trusted Network Service Center, Security Management Commitment will come to a resolution.

Detailed process:

Approval process:

(1) The members of EV CPS Compilation Group compile or modify EV CPS;

(2) Submit EV CPS to departments of CNNIC Trusted Network Service Center for evaluation after the completion of compilation or modification of EV CPS;

(3) Submit the EV CPS that have passed discussion to Security Management Committee, CNNIC Trusted Network Service Center for evaluation or approval in writing;

(4) After EV CPS has passed the evaluation or approval in writing made by Security Management Committee, CNNIC Trusted Network Service Center, it can be issued outside.

1.9 Right to Interpret EV CPS

CNNIC Trusted Network Service Center shall have the final right to interpret this EV CPS.

The agents or employees of CNNIC Trusted Network Service Center have no right, on behalf of the Center, to make any statement on the meaning or interpretation of this EV CPS, unless otherwise authorized by the Center.

1.10 Correspondence with Application Standards

The clauses in this EV CPS conform to the industry standards, including WebTrust audit standards of AI CPA/CICA, EV Certificate Statement of CA/Browser Forum as well as other relevant CA practice standards.

In CNNIC Trusted Network Service Center, the independent audit authority will carry out WebTrust audit on AICPA/CICA each year. The audit subject each year covers but not limited to:

- Disclosure of CA practice
- Integrity of services
- CA environment control

CNNIC Trusted Network Service Center issues and manages EV Certificate under *EV Guideline* issued on the Website http://www.cabforum. If inconsistence arises between the

clauses of *EV Guideline* and this document, *EV Guideline* shall prevail.

1.11 Digital certificate Policy Overview

The digital certificate is a series of data marking the identity information of all communications parties in the internet communications. It is a document that contains the public key and its owner under the digital signature of Certification Authority. The certificate allows the holder to show its identity to the other party in the information interaction, which plays a role of digital identity marking card in the exchange environment.

The Extended Verification Certificate (EV Certificate) contains the information designated in *EV Guideline* and such information has been checked in accordance with standards of *EV Guideline.*

1.12 PKI architecture of CNNIC Trusted Network Service Center

CNNIC Trusted Network Service Center usesChina Internet Network Information Center EV Certificates Rootas root certificate to issue EV Certificate.

Architecture of EV Certificate:

China Internet Network Information Center EV Certificates Root (fingerprint: 4f 99 aa 93 fb 2b d1 37 26 a1 99 4a ce 7f f0 05 f2 93 5d 1e

effective until AAUG 31, 2030). China Internet Network Information Center EV Certificates Root Certificate can be accessed through http://www.cnnic.cn/download/cert/CNNICEVROOT.cer for the fingerprint and effective period of such Certificate.

And subca root CNNIC EV SSL Certificate can be accessed through http://www.cnnic.cn/download/cert/CNNICEVSSL.cer for the fingerprint and effective period of such Certificate.

1.13 Complaint processing procedure

The Employees of CNNIC Trusted Network Service Center will deal with all complaints in the oral or written form as soon as possible and will give a detailed reply within five working

days. If they fail to give a detailed reply within five working days, they will give a brief reply to the Complainant. Where available, the employee of CNNIC will contact will the Complainant by telephone, email or letter immediately after the receipt of such complaint and confirm its receipt of such complaint and give a reply.

2. Technology

This Chapter intends to give an explanation to the architecture of CNNIC Trusted Network Service Center and technical parts of PKI service system.

2.1 Architecture of CNNIC Trusted Network Service Center

Reliable architectural system is adapted in CNNIC Trusted Network center so to provide certificate services. Such system includes computer hardware, software, procedure as well as risk prevention measures and regulations on security risk prevention, in order to improve the availability, reliability, and operation accuracy of the whole system and achieve a reasonable security level.

2.1.1 Term of key pairs

The term of public key and private key of root certificate and intermediate root certificate of CNNIC Trusted Network Service Center shall conform to strict provisions, i.e. the term of key of root certificate is twenty years and that of intermediate root certificate is ten years.

2.1.2 Protection of key

The hardware cryptography module adopted by CNNIC Trusted Network Service Center is a security product that has passed the evaluation made by China national competent authority of cryptography. It is completed by an encryption engine that conforms to relevant provisions issued by the State. Such encryption engine is used to generate, store and utilize root key pairs. The length of root key pairs of CNNIC Trusted Network Service Center is 2048 bits. The hardware cryptography module is set in the security area and the key stored

in the encryption engine can be accessed only in the presence of at least three encryption engine managers (key managers).

The key of root certificate of CNNIC Trusted Network Service Center is not hosted in other organizations. CNNIC Trusted Network Service Center will not accept the trusteeship of signed private key of certificate applicant.

The key stored in the encryption engine can only be accessed only in the presence of a majority of managers. The security of key in the encryption engine can be guaranteed by hardware devices that have passed China national competent authority of cryptography and protection measures that conform to relevant specifications.

Specifically, CNNIIC Trusted Network Service Center adopts authority management policy of five-person control and essential presence of three persons for the protection of private key of root certificate and intermediate root certificate.

2.1.3 Recovery of key

There must be three password cards of encryption engine managers for the recovery of the engine so to back up and recover the engine.

The practice continuity plans include response plan to deal with key disclosure. These plans will be rechecked each year.

If disclosure occurs to private key information of root certificate or intermediate root certificate of CNNIC Trusted Network Service Center that is used to issue domain name certificate, CNNIC Trusted Network Service Center will timely publish. In case such case happens, CNNIC Trusted Network Service Center shall timely terminate the certificate issued under such private key and issue another new certificate to replace it.

2.1.4 Key generation

The key of root CA is directly generated by hardware encryption device and directly stored in a hardware encryption device (encryption engine). CNNIC Trusted Network Service Center uses the encryption hardware device that has passed the certification made by China National Commercial Encryption Management Committee. The key can only

generated by encryption hardware device after three among five encryption engine managers access at the same time. There is no way for one person to execute the operation to generate key. The access of key managers adopts the form of IC card. There is no way for other people to obtain IC cards or relevant passwords.

The key pairs in operating CA is generated in the local hardware encryption device (The hardware encryption device is the one that has passed the certification of China National Commercial Encryption Management Committee) and private key can not generate such encryption hardware device. The key can only generated by encryption hardware device after three among five encryption engine managers access at the same time. There is no way for one person to execute the operation to generate the key. The access of key managers adopts the form of IC card. There is no way for other people to obtain IC cards or relevant passwords.

Certificate applicant: Generated in the terminal of certificate applicant, the signature key pairs adopt strict and safe control measures. CNNIC Trusted Network Service Center does not provide key generation services to certificate applicants. It does not provide key media for them, either.

2.1.5 Key archiving

After the termination of key pairs of root certificate, these key pairs will be archived and stored for at least ten years. The archived key pairs will be kept in the hardware encryption module that conforms to national standards. The key management strategy and procedure of CNNIC will prevent archived key pairs from returning to production system. After the archived key pairs exceed the date of archiving and storage, CNNIC Trusted Network Service Center will revoke them under the provisions of Section 2.1.8, EV CPS.

2.1.6 Key backup

There must also be three password cards of managers needed in the backup of encryption engine so to back up and recover the engine. As one measure to perform disaster recovery, key recover backup is needed. CNNIC Trusted Network Service Center makes encryption

and backup on root certificate and intermediate root certificate by hardware encryption module that conforms to national provisions and the backup copy is stored in an independent system of hardware encryption module so to prevent theft. In the key backup, the password IC card must be used by key managers to start the key management procedure and complete the execution of key backup directions.

The key of certificate applicant is stored in the terminal of certificate applicant, who will adopt appropriate measures to store, back up and recover its key according to the actual situations.

2.1.7 Key alternation procedure

For the Certification Authority with certificates generated by CNNIC Trusted Network Service Center and used to issue and certify the CA, the term of root key and certificate will not exceed twenty years. The root key and its certificate of CNNIC Trusted Network Service Center will be updated within three months before the expiration of them. After alternating to a new root key, the relevant root certificate will also be issued to the public for use. The original root key will be kept for a certain period so to verify the certificate with the signature of the original root key.

2.1.8 Key Revocation

The root certificate and intermediate root certificate of CNNIC Trusted Network Service Center will be archived and stored for ten years until they have become invalid and appropriate measures will be taken to revoke them. After the end of archiving term of archived key, it shall be securely revoked with the involvement of several trusted personnel. The key revocation ensures that its private key will be completely deleted from the hardware encryption module and there will be no information left.

The private key of certificate applicant will be stored in the terminal of certificate applicant. After the termination of its certificate, it shall be immediately revoked by the certificate user on its own.

2.1.9 Issue public key of CA root to certificate users

CNNIC Trusted Network Service Center will issue its public key on the website so to be convenient for certificate users to obtain.

The managers operate the certificates and the archiving of public key of CNNIC Trusted Network Service Center.

2.1.10 Physical operation of CNNIC Trusted Network Service Center

2.1.10.1 Physical address

CNNIC Trusted Network Service Center operates in the location under reasonably safe conditions. During the construction of sites, the Center has adopted appropriate prevention measures so to make a good preparation for the operation of CNNIC Trusted Network Service Center

2.10.1.2 Access control

The personnel of CCNIC Trusted Network Service Center who have access to the key area, control encryption or other operation procedures and may cause serious impact on the issuance, use and termination of EV Certificate shall be deemed to carry on trusted responsibility. Such personnel include but not limited to system manager, operator, encryption engine manager, engineer and administrative personnel that are delegated to supervise the operation of CNNIC Trusted Network Service Center.

CNNIC Trusted Network Service Center has formulated relevant management rules for the personnel that have relation to domain name certificate services of CNNIC Trusted Network Service Center and carry on trusted responsibility, which include:

- Formulation of operation and control procedures of entities and systems at all levels according to role and responsibility
- Detailed responsibility division provisions

CNNIC Trusted Network Service Center carries out reasonable security control, limits the access to hardware and software of the Center (including server, workstation and any outer

encryption hardware module). The personnel who have access to the above hardware and software only limit to the ones who carry out trusted responsibility under the provisions of this CPS. They carry out control and digital monitoring on such access so to prevent invasion without authorization.

CNNIC Trusted Network Service Center ensures there will be at least two personnel in the processing and approval of EV Certificate request before the generation of EV Certificate.

2.1.10.3 Transmission of documents and materials

The transmission of all documents among CNNIC Trusted Network Service Center, its Registration Authority (RA) and Local Registration Authority (LRA) are carried out in a safe and controlled way.

2.1.10.4 Power and air-conditioning

The power and air-conditioning resources available for CNNIC Trusted Network Service Center include dedicated air-conditioning system, Uninterruptible Power Supply (UPS) and generator car rented from Power Company in order to prepare supplying power in case of power system failure in the urban area.

2.1.10.5 Natural disaster

The facilities of CNNIC Trusted Network Service Center can be prevented from natural disasters within the possibly reasonable extent. CNNIC Trusted Network Service Center has prepared proper fire prevention plans and fire-fighting system for its facilities.

2.1.10.6 Fire prevention and protection

CNNIC Trusted Network Service Center has prepared proper fire prevention plans and fire-fighting system for its facilities.

2.1.10.7 Media storage

Media storage and processing procedures have been well prepared.

2.1.10.8 Offsite backup

Appropriate preparations and offsite storage have been made for the system data of CNNIC Trusted Network Service Center so to acquire enough protection and prevent theft, damage and media decay.

2.1.10.9 Print Documents storage

Print documents (including identity confirmation files and management documents of certificate holder) are well stored by CNNIC Trusted Network Service Center and can only be read by authorized personnel within the permitted authority.

2.1.10.10 Waste material disposal

Dispose of waste material according to normal waste material disposal procedure. The encrypted devices shall be physically damaged or reset according to the instruction of device manufacturers before they become invalid.

2.1.10.11 Electromagnetic Protection

To prevent internal information leak from electromagnetic radiation, and also shielding the electromagnetic interference, CNNIC CA build a Electromagnetic Shielding room, and passed the Chinese Military C level authentication which is stable and safety.

All CA server and CA encryption machine of CNNIC CA are deployed in the Electromagnetic Shielding room.

2.1.10.12Other security procedures

CNNIC Trusted Network Service Center executes a set of complete and reasonable security procedures which are used to:

1. Protect all data, software, keys and procedures in the process of EV request, certificate

approval and issuance;

2. Prevent predictable threats in the integrity, confidentiality and availability of EV data;

3. Prevent unauthorized or illegal access, utilization, disclosure, modification or damage to any EV data;

4. Prevent some disastrous damage or injury to EV data or EV procedures;

5. Abide by other security demands of CNNIC Trusted Network Service Center that conform to laws.

The security procedures of CNNIC Trusted Network Service Center include regular risk assessment:

6. Recognize predictable threats from the outside and inside, e.g. unauthorized access, disclosure, wrong use, modification or damage to relevant data concerning EV;

7. Evaluate the consequences caused by these potential threats;

8. Evaluate whether CNNIC Trusted Network Service Center has taken or formulated measures and policies.

CNNIC Trusted Network Service Center, based on risk evaluation, has relevant implementation measures to ensure the continuity and effectiveness of EV Certificate Policy.

2.1.11 Annual assessment

CNNIC Trusted Network Service Center carries out annual assessment each year so to ensure that normal operation process conforms to security policy and other procedure control.

2.2 Digital certificate management

The certificate management of CNNIC Trusted Network Service Center includes but not limited to the following parts:

- Verification on the identity of certificate applicants
- Certificate issuance
- Certificate revocation

- Certificate distribution
- Certificate publication
- Certificate backup
- Certificate retrieval according to special usage purposes
- Verification on domain names of applied certificates
- Verification on authorization of entity to issue EV certificate

2.3 Repository of CNNIC Trusted Network Service Center

CNNIC Trusted Network Service Center maintains a repository, which includes Certificate Revocation List (CRL) issued by the latest root and intermediate root, root certificate, CPS, EV CPS, CP, EV CP documents and other relevant materials of CNNIC Trusted Network Service Center.

Except for regular maintenance and emergency repairs for at most four hours each week, the storage pool keeps open for 24 hours each day and seven days each week. The storage pool of CNNIC Trusted Network Service Center can be accessed through the following URL: http://www.cnnic.cn/index/0T/index.htm

The content of storage pool can be altered according to alternations. The published materials and data are available to all internet users; however, they can only be updated by the managers of CNNIC Trusted Network Service Center.

2.4 Certificate type of CNNIC Trusted Network Service Center

With the development of business, CNNIC Trusted Network Service Center may extend its production line, including issued certificate type. For the issuance of each new certificate product, CNNIC Trusted Network Service Center will issue another new CPS within seven days before the provision of new Certificate Practice.

The current issued domain name certificate brands include:

“Trusted EV server certificate”, which is divided into:

- ◆ Single domain name certificate: The CN of certificate subject is a fixed domain name;
- ◆ Multiple domain name certificate: The CN of certificate subject is multiple parallel

domain names, such as “CN=a. xxx.xxx，CN=b. xxx.xxx，CN=c. xxx.xxx”. SA extension includes these multiple domain names.

The trusted EV server certificate issued by CNNIC includes but not limited to domain name certificates, which can not be used for other purposes.

2.5 Term of EV certificate

The term of EV Certificate of new applicant under this EV Certificate Practice Statement shall be one or two years.

The term of EV Certificate of new applicant under the provisions of certificate renewal procedures in this EV Certificate Practice Statement shall not exceed the above term. The term will be marked in EV Certificate.

2.6 Extension and nomination

2.6.1 Extension of digital certificate

The domain name certificate issued by CNNIC Trusted Network Service Center is of extensive universality. The format of certificate conforms to X.509 V3 standard and it can provide the capability to support certificate extension.

2.7 Private key generation and certificate request process of certificate applicant

2.7.1 Generation of private key

The signature private key pairs are generated in the terminal of client. CNNIC Trusted Network Service Center has formulated strict and safe control measures and the private key pairs can be generated by intelligent IC card, other hardware encryption devices or encryption software, but CNNIC Trusted Network Service Center does not provide the generation, backup and recovery services. In the process of application, the certificate applicant will submit CSR that contains public key and detailed enterprise information.

2.7.2 Requirements on Document

Before the issuance of EV Certificate, the certificate applicant must submit the following documents to CNNIC Trusted Network Service Center:

- Application Form of EV Certificate
- User Agreement
- Other documents made by CNNIC Trusted Network Service Center according to *EV Guideline*

2.7.3 Requirements on the role of applicant

The EV certificate application unit needs to play the following role and the details may be adjusted:

- Certificate applicant
- Approver for Certificate application
- Agreement signer: The agreement on EV certificate application must be signed by the authorized personnel.
- Applicant Representative: In the case where CA and Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the applicant, employed by the applicant, or an authorized agent who has express authority to represent the applicant , and who has authority on behalf of the applicant to acknowledge and agree to Terms of Use.

The certificate applicant can authorize one or four persons to fulfill all roles. The applicant of EV Certificate shall be a natural person with authorization. Also, it shall be the employee of application unit or authorized agent (certification materials of the application unit or the third party are required).

2.7.4 EV Certificate application request

- Summary: The operator to apply for EV Certificate must submit its application to the

LRA of CNNIC Trusted Network Service Center designated by CNNIC or RA of operation mechanism designated by CNNIC. CNNIC is not oriented for the applicant to accept the application.

- Content of request: The EV Certificate Request must contain an application signed and confirmed by the applicant or its authorized representative. The applicant also needs to submit an agreement signed by the applicant or its authorized representative, including the confirmation on the accuracy and correctness of information contained in EV Certificate.
- Information requirement: The EV Certificate Request may include all actual information of application units as shown in the Certificate, and other information of applicant required by CNNIC Trusted Network Service Center under *EV Guideline.* To prevent that EV certificate request fails to contain necessary information or verify the relevant information further, CNNIC Trusted Network Information Center will obtain other information from the certificate applicant and agreement signer.

  The applicant information shall include but not limited to the parts of this *EV Guideline*.

2.8 Protection and backup of private key for certificate applicant

The private key of applicant is generated in the terminal of client and is of strict and safe control measures. CNNIC Trusted Network Service Center does not provide services on the generation, backup and recovery of private key.

CNNIC Trusted Network Service Center strongly proposes that the applicant use password, intelligent IC card and other hardware encryption devices or encryption software to avoid illegal access or use of private key.

2.9 Transmission of public key for certificate applicant

The certificate applicant uses security software at the terminal of server to transmit the public key to CNNIC Trusted Network Service Center for the generation of Certificate. Such request (CSR) uses the format of PKCS#10 with the digital signature and can be submitted through the CNNIC website (https://rawhois.cnnic.cn/pages/CertDownloadStart.ftl).

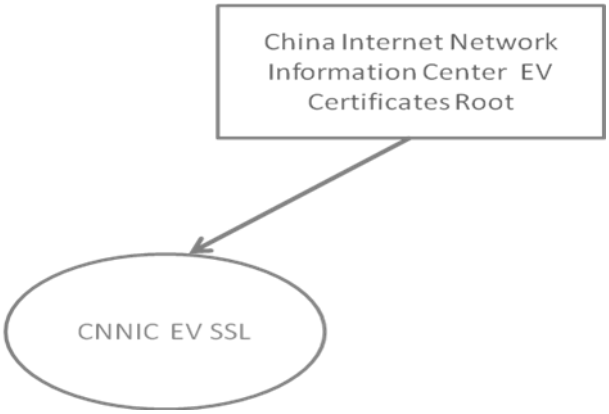
2.10 Transmission of issued certificate

After CNNIC Trusted Network Service Center approves such certificate application, it will send Reference No. and the first 13 bits of Authorization Code by email and the last 3 bits by phone to the operator for certificate application.

2.11 EV Certificate architecture of CNNIC Trusted Network Service Center

EV certificate architecture of CNNIC Trusted Network Service Center:

2.11.1 Structure of EV certificate root



Root structure diagram

2.11.2 Relevant instruction to EV root CA certificate

The root CA certificate does not contain fields of certificatePolicies or extendedKeyUsage extensions.

The application software distributor or any certificate relying party may confirm the approved and signed root CA of EV certificate through the storage of EV data identifier concerning root CA certificate.

For its key extensions, the parts of CA domain have been set “TRUE”. Meanwhile, pathLenConstraint is not expressed.

2.11.3 Content and subject of certificate

Under *EV guideline*, the basic requirements on EV Certificate contents include:

Information of subject organization

(a) Name of organization

Certificate domain subject: OrganizationName（OID:）

Compulsory/optional: Compulsory

Content: This part contains the name of certificate holder of CNNIC after passing the recording or document verification of official organizations. The name must be a full name of legal unit and the maximum length of the name shall not exceed 64 characters. If there are more than 64 characters, abbreviation or omission of words without great influence can be adopted.

(b) Domain name

Subject of certificate domain: CommonName

Compulsory/optional: optional

Content: CN is parallel multiple domain names in EV multiple domain name certificate and single domain name certificate is a single domain name. EV Certificate does not provide wild-card certificate type.

(c) Business type

Subject of certificate domain: businessCategory

Compulsory/optional: compulsory

Content: The business type field of CNNIC Trusted Network Service Center includes private organization (v1.0, Cause 5.(b)), government entity (v1.0, Cause 5.(c)), commercial entity (v1.0, C, Cause 5.(d)) and non-commercial entity (v1.0, C, Cause 5.(e)).

Definition of private organization: individual industrial and commercial, foreign-invested enterprises

Definition of government entity: government authority, institution

Definition of commercial entity: legal person of enterprise

Definition of non-commercial entity: social club and others

(d) Established or registered region

Certificate domain: established/registered location (state, province and municipality) used to determine whether the subject is a national, provincial or city level unit

Compulsory/optional: compulsory

Content: irrelevant information shall not be included. E.g. the fields of province and municipality may not be filled for national-level unit; the field of municipality may not be filled for provincial unit. For provincial, municipal and national regions, only English letters can be input instead of Chinese. The national region is CN in default. For cities and provinces of other locations, Chinese may be input.

(e) Registration No.

Subject of certificate domain: serialNumber

Compulsory/optional: compulsory

Content: For private organizations, Registration No. distributed by the authority of its establishment or registration. If there is no registration no., the date of establishment or registration can be filled.

For government entity, input relevant words to indicate the identity of the subject.

For commercial entity, input the registration no. acquired after the approval of government. If there is no registration no., fill in the date of establishment.

(f) Operation and business address

Subject of certificate domain: country, state or province, city/town, Street No. and postal code.

Compulsory/optional: The country, state or province and city/town are compulsory and the Street No. and postal code are optional.

Content: physical operation address of subject.

2.11.4 Extended options of key usage

The certificate format used by CNNIC Trusted Service Center is X. 509 (Version 3). The key extended options of EV Certificate are used to identify the usage and technical requirement of Certificate.

The extended options of EV Certificate of CNNIC Trusted Network Service Center are as

follows:

Root CA certificate

- Basic constraint: This extended option must be critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.
- Key usage: “key” field. Key usage in the limited certificate. KeyCertSign and cRLSing must be set.

Sub CA certificate

- CertificatePolicies: This extended option must exist and may not be marked as key extension. Name of publishing site= CCL publishing site HTTP URL.
- authorityInformationAccess: This extended option should exist, and may not be marked as key extension. It should include OCSP response address of CNNIC Trusted Network Service Center (HTTP URL).
- Basic constraints: This option is set “True” and the extended option is marked as “key”.
  Subject Type=CA
  Path Length Constraint=None
- Key usage: This option must exist and be marked as key. CertSign and CRLSign must be set and other options must be set.

User certificate

- CertificatePolices: This extended option must exist and can not be marked with key.
  Certificate Policy:
  Policy Identifier=EV Policy OID=1.3.6.1.4.1.29836.1.10
  Policy Qualifier Info:
  Policy Qualifier Id=CPS
  Qualifier:
  http://www.cnnic.cn/cps/
- CRLDistributionPoint: Such extended option exists and is marked as key. It contains the issuance of Certificate Revocation List (CRL) of CNNIC Trusted Network Service Center (HTTP address: URL=http://www.cnnic.cn/download/evcrl/crl1.cr)

AuthorityInformationAccess: Such extended option exists and is not marked as key.

[1] Authority Info Access

Access Method=OCSP (1.3.6.1.5.5.7.48.1)

Alternative Name:

URL=http://ocspev.cnnic.cn

[2] Authority Info Access

Access Method=CA Issuer (1.3.6.1.5.5.7.48.2)

Alternative Name:

- URL=http://www.cnnic.cn/download/cert/CNNICEVSSL.cer

Basic constraints: exist; Path Length Constraint is set to be null.

- Key usage: exist; KeyCertSign and cRLsign are not set.
- ExtKeyUsage: The value for id-kp-serverAuth is 1.3.6.1.5.5.7.3.1.

2.11.5 EV Certificate Policy

The Certificate Policy explains in detail CNNIC Trusted Network Service Center's rule and request to issue and manage certificate. The Certificate Policy is formulated by certificate issuing authority and extensively issued to the outside. Meanwhile, OID conforming to the application standard is applied to International Standard Organization so to ensure its compatibility with other applications. OID is transmitted in the communication services. As the identifier of certificate policy of this Certificate Authority, it provides relevant policies about certificate services on behalf of Certification Authority. Besides, only when the certificate applicant agrees with the Certificate Policy, it can apply for and obtain digital certificate from CA.

- EV User Certificate

Each EV Certificate issued by CNNIC Trusted Network Service Center contains an OID defined by CNNIC Trusted Network Service Center. Such OID is in the extended option of certificatePolicies of certificate, which is used to: (1) indicate the type of CA policy of this certificate; (2) show CNNIC Trusted Network Service Center's conformity with *EV guideline;* (3) mark the certificate as EV Certificate through the previous agreement with software application vendor.

- EV Sub CA Certificate

Temporarily, CNNIC Trusted Network Service Center provides no services about issuance of certificate to CA.

- Root CA Certificate

CNNIC Trusted Network Certificate does not include certificatePolicies or extended fields to extend the usage of terminal key.

2.11.6 Encryption algorithm and key length

The key pairs of root certificate and intermediate root certificate in CNNIC Trusted Network Service Center are RSA of 2048 bits. The key pairs of certificate applicant are also required to be RSA of 2048 bits.

Format for EV Certificate of CNNIC Trusted Network Service Center:

EV Certificate of CNNIC trusted server		
Signature algorithm	Sha1RSA	
Issuer	CN	CNNIC EV SSL
	O	China Internet Network Information Center
	C	CN
Period of validity	One year , two years	
Subject	CN	Domain name
	OU	Name of department
	O	Name of unit
	L	City
	S	State or province
	C	Country
	Serial No.	Registration No.
Key identifier of issuing authority	KeyID	
Key usage (non-key)	Digital Signature, Key Encipherment (a0)	
intensified key usage	Server verification (1.3.6.1.5.5.7.3.1)	
Basic constraints	Subject Type=End Entity Path Length Constraint=None	
Certificate Policy	[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.29836.1.10 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cnnic.cn/cps/	
CRL Distribution Policy	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=crl* (*Such Serial No. is calculated according to Serial No. of certificate） OU=crl O= China Internet Network Information Center	

	C=cn [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.cnnic.cn/download/evcrl/crl*（*Such Serial No. is calculated according to Serial No. of certificate）.crl
Fingerprint algorithm	sha1RSA

2.12 EV CRL and its architecture of CNNIC Trusted Network Service Center

2.12.1 EV CRL issuance

CNNIC Trusted Network Service Center issues the latest CRL issued by intermediate root to the outside. The access address is:

http://www.cnnic.cn/download/evcrl/crl* (*Such Serial No. is calculated according to Serial No. of certificate). crl

In the storage pool of CNNIC Trusted Network Service Center, CRL issued by intermediate root is updated once every twelve hours.

As intermediate root is not terminated, the address of CRL issued by root is: URL=http://www.cnnic.cn/download/rootcrl/CRL1.crl, which is updated once every six months (182 days). After the termination of intermediate root, CRL issued by root will be immediately updated.

CRL stores all certificate items for five years and the revoked certificate items will not be deleted within five years.

2.12.2 EV CRL architecture

CRL architecture of CNNIC Trusted Network Service Center:

Version	Indicate Version No. of CRL	X.509 (Version 2)
Signature	Signature of CA issuing CRL	CN = CNNIC EV SSL O = China Internet Network Information Center C = CN
algorithmIdentifier	Define the algorithm for issuance of CRL	
Issuer	Distinguished name of CA issuing CRL	

thisUpdate）	Issuance time of CRL
next update	Estimated update time of next CRL
revoked certificates	CRL entrance
	Serial No. of Certificate
	Revoked date

2.13 Online Certificate Status Protocol (OCSP)

2.13.1 OCSP issuance

Whether the relying party makes inquiry on online status depends on its security requirement. For the application with high demand on security guarantee and complete reliance on certificate to conduct identity recognition and authorization, the relying party may examine the status of such certificate through OCSP system before trusting a certificate.

CNNIC Trusted Network Service Center provides Online Certificate Status Protocol (OCSP) service based on the certificate status of HTTP. Such service is available for 7*24 hours except for emergency and regular maintenance for at most four hours each week. When the user clicks on the certificate status response through OCSP, it will see the specific time for the next update of such certificate status (According to different certificates and roots, the certificate is updated once within 12 hours and root certificate is updated once within 120 days) and all certificate items are stored in OCSP.

2.13.2 OCSP structure

The OCSP issued by CA of CNNIC Trusted Network Service Center shall conform to RFC2560. The OCSP response shall contain at least the basic domains and contents as provided in the following table.

Basic domains of OCSP structure

Domain	**Value or value constraints**
Status	Response status, including success, error request format, inner errot, later retry, request without signature and requested signature certificate without authorization. When the status is ok, the following items shall be included.
VFersion	V1
Signature algorithm	Algorithm for OCSP issuance. Use sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) for signature.
Issuer	Entity issuing OCSP. SHA1 Data abstract value and distiguhished name of certificate for public key of issuer.
Time of	OCSP Response generation time

generation	
Next update	(According to different certificates and roots, the certificate is updated once within 12 hours and root certificate is updated once within 120 days)
Certificate status list	Include certificate status list inquired in the request. Each certificate status includes certificate identifier, certificate status and certificate termination information.
Certificate identifier	Includes data abstract algorithm, data abstract value for distinguished name of certificate, abstract value of public key and Serial No. for certificate
Certificate status	Latest status of certificate, including valid, terminated and unknown.
Certificate termination information	Contain time and reason for termination when the returned certificate status is terminated.

2.13.3 OCSP request

The OCSP request may support two methods, GET and Post. If the request information is less than 255 bytes, GET can be used. If the request information is more than 255 bytes, POST method shall be used.

The request information shall at least contain:

Version of agreement;

Service request;

Identifier of object certificate;

Extended option required by OCSP server.

Notice to expiration time: The longest expiration time of information that OCSP feedbacks is ten days. All users who confirm the effectiveness of certificate through this information shall pay attention to expiration period.

2.13.4 OCSP response

The correct OCSP response shall include:

Version of response agreement;

Name of OCSP server;

Response to each certificate in a request (including identifier of object certificate, status value of certificate, duration for valid response and optional extended option);

Optional extended item;

Optional extended option;

Signature calculation method OID;

Signature calculated through hash function.

2.14 Security control

2.14.1 Computer security control

Operated in a safe environment, CNNIC Trusted Network Service Center adopts partition access authority control. The separation between core system and other systems adopts firewall and infringement check security control. Meanwhile, it adopts:

1. System security configuration; shut down unnecessary services and ports.
2. The latest patch procedure shall be installed in the operation system and special persons are responsible for the installation of the latest patch.
3. The special person shall be in charge of each machine in the production system. It shall strictly abide by operation procedures and passwords are managed and authorization is given level by level. Each person shall be responsible for the operation within the range of authority.
4. Audit system of log and operation records.
5. Data backup and recovery mechanism.

2.14.2 Security control of Life duration technology

The system used by CNNIC Trusted Network Service Center is carefully tested prior to their use and irregular check is carried out in the process of utilization.

2.14.3 Network security control

The system of CNNIC Trusted Network Service Center is divided into different sections according to different security requirements. Offline operation is adopted for parts of high security level system. And hierarchical model is adopted to guarantee the security of network and reliability of system.

3. Organizational architecture

The Certificate Practice of CNNIC Trusted Network Service Center is performed under safe environment. This Chapter mainly intends give a summary to security policy, mechanism of physical and logical access, service level and employee strategy so to provide reliable certificate practice.

3.1 Conformity with EV certificate practice statement

CNNIC Trusted Network Service Center provides practice, operation and services under this *CNNIC EV Certificate Practice Statement*.

3.2 Termination of practice for certificate issuing authority

Once CNNIC Trusted Network Service Center needs to terminate certificate practice due to any reason, it will timely issue a notice on its website, etc. and provide the consecutive services including responsibility of certificate holder, records keeping and recovery, etc. Before the termination of certificate practice, CNNIC Trusted Network Service Center will perform the following operations.

- In case of the termination of services for CNNIC Trusted Network Service Center, the Center will terminate all certificates issued by it and hand the filing records over to the relevant authority in accordance with laws and regulations.
- After the termination of services, CNNIC Trusted Network Service Center will store the records of Certification Authority for ten years (as of the termination of services). These records include root certificates, intermediate certificates; issued domain name certificates, certificate practice statement and Certificate Revocation List (CRL) (CP and statement are different).

3.3 Format of records archiving

CNNIC Trusted Network Service Center will perform archiving of materials and records, as

well as make and store the duplicated copy of filing materials and records.

The archived materials are clearly marked with the initial date and time of archived projects. CNNIC Trusted Network Service Center will prevent from adjusting the system clock with authorization by control measures.

3.4 Retention period for records archiving

CNNIC Trusted Network Service Center must ensure that the archived records shall contain enough materials so to determine whether the certificate is valid and the previous is proper. Under the requirement of *EV guideline*, CA must keep all documents and EV certificate that relate to the EV certificate request and certification. CNNIC Trusted Network Service Center shall keep the following data:

- System device structure records
- Evaluation results and device eligibility recheck records
- *Certificate Practice Statement*(all versions)
- Binding agreement on CNNIC Trusted Network Service Center
- All issued EV certificate, revoked EV certificates and Certificate Revocation List (CRL)
- Regular records of events
- EV certificate request and all documents in the process of verification
- Other work logs used to verify the content for archiving
- Archiving of relevant technical documents on system introduction

The above archived records are properly stored for at least ten years. The audit tracking documents are stored in an appropriate way that CNNIC Trusted Network Service Center proposes. All records will be archived in a safe place.

3.5 Core function log

Under the requirement of *EV guideline*, CNNIC Trusted Network Service Center will keep all log records, including EV certificate request, disposal and all logs in the process of issuance. Time, data and operation records of personnel needs to be recorded in the log.

The archived media stored in CNNIC Trusted Network Service Center are protected by all

kinds of objects or encryption measures, so to prevent entry without authorization. The protection measures are used to protect archived media from environmental damage including temperature, humidity and magnetic field. When the movable storage media is about to terminate its life period, security data damage devices of third parties are used to clear these data.

The archived records include but not limited to the following events:

- Key life period management of CNNIC Trusted Network Service Center, which includes:
  - Key generation, backup, storage, backup, archiving and revocation;
  - Password device statement period management events.
- EV Certificate statement period management events of CNNIC Trusted Network Service Center, which includes:
  - EV Certificate request, renewal; key reapplication and revocation;
  - All verification activities under this Guideline;
  - Verification on data, time, used telephone, calling object and final results of verified telephone;
  - Receiving and rejection of EV Certificate request;
  - Issuance of EV Certificate;
  - EV Certificate Revocation List (CRL) and OCSP item
- Security events, which include:
  - Successful and failed PKI system access trial;
  - Implemented PKI and security system activities;
  - Alternation of security policy;
  - System collapse, hardware failure and other abnormal phenomena;
  - Firewall and route activities;
  - Item of CA device and its exit from it
- Access item must contain the following elements:
  - Data and time of item;
  - Identity for personnel who make logs;
  - Description on item.

3.6 Practice continuity plan and disaster recovery

To ensure the completeness of services, CNNIC Trusted Network Service Center will implement record and test in phase the continuity of testing practice and disaster recovery plan. Such plan needs to be updated or modified at least once for each year.

CNNIC Trusted Network Service Center has made proper practice continuity plan, which includes daily backup of main practice information and CA system data and proper backup of CA system software so to maintain the continuous operation of main practice and guarantee the provision of services or recovery of services at the shortest time under the impact of serious failure or disaster.

CNNIC Trusted Network Service Center does not provide any disaster recovery base in an offsite. In case of serious failure or disaster, CNNIC Trusted Network Service Center will give a notice to government authorities in time and publish the operation transition from production base to disaster recovery base.

Upon the occurrence of disaster and prior to the re-building of reliable environment:

- Sensitive materials or devices will be safely locked in the facility;
- If Sensitive materials or devices are unable to be safely locked in the facility or there is risk for these materials or devices to be damaged, they will be moved from the facility and locked in other temporary facilities.
- Access control will be adopted for the access of facility so to prevent theft or access without authorization.

3.7 Availability of revoked data

CNNIC Trusted Network Service Center issues EV Certificate Revocation List for the relying party to certify the effectiveness of EV digital certificate issued by CNNIC Trusted Network Service Center. EV CRL includes the access inlet of revoked EV certificate and 24 hours is available for access. For intermediate root, CNNIC Trusted Network Service Center issues CRL once every twelve hours. If intermediate root is not terminated, the CRL issued by root is updated every six months (182 days). After the termination of intermediate root, the CRL issued by root will be immediately updated. The terminated CRL list needs archiving and

kept for ten years.

3.8 Issuance of key information

CNNIC will issue *EV Certificate Practice Statement* and agreement with users, etc. on its official website. All updates and modifications will be strictly executed in accordance with this *EV Certificate Practice Statement.*

3.9 Confidential Information

CNNIC Trusted Network Service Center will ensure the security and confidentiality of user information or confidential information in accordance with provisions of this *EV Certificate Policy Statement.*

3.9.1 Type of confidential information

CNNIC Trusted Network Service Center lists the following information as confidential and has taken proper measures to ensure that confidential information is not disclosed.

a) The special information managed and controlled by CNNIC Network Service Center will be secretly kept by the Center; unless otherwise stated by law, disclosure to the outside shall not be allowed.

b) Except the information issued in EV certificate, EV CRL, EV certificate policy and EV CPS, the information about certificate holder is confidential information; unless otherwise requested in certificate policy or stated by law, it shall not be opened to the outside.

c) The documents and materials submitted by certificate applicant include signed agreement, identity certification as well as documents and materials needed to be submitted by the applicant (No matter whether passing evaluation or not).

d) Generally, the annual audit result shall be kept confidential, unless CNNIC Trusted Network Service Center Security Management Committee thinks it is necessary to publish the result for audit.

e) Practice continuity plan and disaster recovery plan.

f) Architecture of CNNIC Trusted Network Service Center, certificate management,

registration service and operation records of data.

3.9.2 Non-confidential Information

a) The information that is contained in EV certificate and EV CRL issued by CNNIC Trusted Network Service Center is non-confidential.

b) The information in EV CPS that is published by CNNIC Trusted Network Service Center is non-confidential (or other commercial matters published).

c) The termination reason is listed in EV CRL when CNNIC Trusted Network Service Center terminates one EV certificate. The code for the termination reason is non-confidential information and all the other EV certificate holders and EV certificate relying parties can share such information. However, other details about termination are not published in general.

CNNIC Trusted Network Service Center will publish information in accordance with law and enforcement requirements of law enforcement officials.

CNNIC Trusted Network Service Center will request the information holder to publish the information about the holder in accordance with the requirements of information holder.

3.9.3 Confidential information access

Only authorized personnel can access the confidential information. The employee of CNNIC Trusted Network Service Center needs to abide by the relevant provisions.

3.10 Computer security audit procedure

3.10.1 Type of recorded events

The important security events of CNNIC Trusted Network Service Center will be manually or automatically recorded in the audit tracking records under protection. These events include but not limited to the following:

- Suspicious network activities
- Attempts to entry and failure to access

- Events about the installation of devices or software, modification and configuration of CNNIC Trusted network Service Center system
- Process for relevant personnel to access all parts of CNNIC Trusted Network Service Center

The operations for regular management of EV certificate are also included in the audit tracking records and these operations include but not limited the following:

- Disposal of request on the termination of EV certificate
- Actual issuance (including certificate registration, renewal and reissuing, etc.) and termination of EV certificate
- Update of storage pool materials
- Compilation of EV Certificate Revocation List and publication of new data
- Key shift of Certification Authority
- File backup
- Emergency key recovery

3.10.2 Times for processing records

CNNIC Trusted Network Service Center will deal with audit tracing records every two weeks in order to audit and track activities, exchanges and procedures about CNNIC Trusted Network Service Center.

3.10.3 Term for storage

The storage period for the audit and tracking records is ten years.

3.10.4 Audit tracking records protection

Multiple person control is performed when CNNIC Trusted Network Service Center disposes of audit tracking records, which can provide enough protections and prevent relevant records from being injured or deliberately modified.

3.10.5 Audit tracking records backup

CNNIC Trusted Network Service Center will make proper backup for the audit tracking records in accordance with procedures. The backup will be stored off the machine and be well protected so to prevent theft, damage and media decay.

3.10.6 Security events notification

CNNIC Trusted Network Service Center has automatic monitoring system, which can report important security events to the relevant responsible persons or systems of CNNIC Trusted Network Service Center.

3.10.7 Vulnerability assessment

The vulnerability assessment is part of risk assessment of CNNIC Trusted Network Service Center: CNNIC Trusted Network Service Center carries out vulnerability assessment concerning technical security and management security and take enforcement measures in accordance with assessment report.

3.11 Employee management and rules

CNNIC Trusted Network Service Center adopts the following rules and management procedures to guarantee the credibility of employees and their fulfillment of relevant responsibilities.

3.11.1 Employee identity verification

CNNIC Trusted Network Service Center (including RA) makes investigation on the background, qualifications and experience, etc. of personnel who carry on reliable responsibilities, which is regularly preformed prior to and after employment according to need. The credibility and competence of employees are verified in accordance with this EV CPS and personnel strategy of CNNIC Trusted Network Service Center: loyal, reliable, with enthusiasm, without performing other part-time job affecting the operation and without

serious error and crime records of the same industry.

Background: High political quality, excellent practice, strong responsibility, strong sense of principle, without crime and illegal records.

Qualifications: Be good at the job; its education, training and work experience can guarantee its competence for the job.

The staff and management policy of CNNIC Trusted Service Center ensures the credibility and competence of the Center or LRA personnel on behalf of it and guarantee that they will Perform their duties in accordance with this EV CPS.

The personnel who fail to pass primary and regular investigation shall not act or carry on reliable responsibility. The investigation includes education, work experience. Such information shall be verified and confirmed by Human Resources.

3.11.2 Training and skills

The employees of CNNIC Trusted Network Service Center (including RA) have received primary training required for the implementation of their responsibilities. CNNIC Network Service Center will provide continuous training so to enable employees to master the required latest working skills. The training includes but not limited to: knowledge to Public Key Infrastructure (PKI), means and procedure of verification, practice schedule, common threats and response measures, etc.

Meanwhile, the employees of CNNIC Trusted Network Service Center (including RA) will receive guide manual, in which registration, renewal, obtaining of two codes, reissuing and termination procedure and other software functions concerning its responsibilities are described in detail.

3.11.3 Separation of duty

CNNIC Trusted Network Service Center has strict management measures so to ensure the independence of employee authority. The verification and issuance of EV certificate application information and certificate are carried out by two roles.

3.12 EV audit

In accordance with relevant provisions, assessment about conformity with regulations is held once at least every twelve months by outer independent audit authority, so to examine whether the system of issuance and termination of EV Certificate and EV Certificate Revocation List issuing EV Certificate are in strict conformity with *EV Guideline*, this EV CPS and control measures relating to CNNIC Trusted Network Service Center.

The audit contains:

1) Published commercial matters;

2) Integrity of services (including control on key and certificate life period management);

3) Environmental control.

The audit result shall be reported to CNNIC Trusted Network Service Center Security Management Committee. CNNIC Trusted Network Service Center will confirm the improvement proposal and adopt improvement actions in accordance with detailed audit comments.

The inner auditor carries out audit on the compliance of practice operation every two weeks and makes self-check on the compliance on approvers and registers.

3.13 Issuance of information

The storage pool of CNNIC Trusted Network Service Center, including EV certificate practice statement, EV certificate policy, etc, will be published on CNNIC Website (www.cnnic.cn). The location of storage pool can be browsed online and can be prevented from any modification without authorization.

4. Practice Statement

This Chapter mainly describes the application process of certificate like application materials required to be submitted. Especially, if the user uses other languages (like English) in its submittal material in the EV certificate application, renewal, and modification operations, RA needs to explicitly express them in such language. The verification

personnel of CA will check the work of RA to verify whether it conforms to the requirements of applicant.

4.1 EV certificate application

It is specially noted in the application of EV certificate for CNNIC Trusted Network Service Center that, when all users fill in the application form for trusted server certificate, if some items are optional and no content needs to be filled, please input null only. The term for EV Certificate is one year or two years. If it is two-year certificate, annual inspection shall be performed during the period of nine to 12 months upon the use of certificate and relevant verification materials shall be submitted as below for such operation.

4.1.1 Single domain name EV Certificate

1. The application operator for EV Certificate submits application materials to the data processor of LRA.

- Identity certification of EV Certificate applicant:
  - Provided by enterprise: duplicate copy of Organization Code Certificate or Enterprise Business License for Enterprise's Legal Person (with each page sealed);
  - Provided by government authority: duplicate copy of Organization Code Certificate (with each page sealed);
  - Provided by institution: duplicate copy of Organization Code Certificate (with each page sealed);
  - Provided by social club: duplicate copy of Organization Code Certificate (with each page sealed);
  - Account opening certificate issued by bank (with each page sealed).
- Original copy of application letter for EV Certificate registration (with each page sealed).
- When the EV Certificate applicant is an enterprise/government authority/institution/social club, the duplicate copies of identity certificates for manager and operator need to be submitted.

2. The data processor for LRA carries out primary verification. It obtains, through domain

name registration inquiry (whois) function, the material for domain name register material of applied EV certificate, check whether the domain name register is identical with the applicant of EV Certificate and determine whether the EV Certificate register actually owns such domain name through primary verification.

(Note: In terms of verifying the identity and legal character of private organization or business entity, its parent, subsidiaries, or affiliates should also be concerned about.)

3. After the primary verification of data processor of LRA is passed, input the above material through RA system; submit the application and all the paper application material to the RA reviewer of CNNIC RA. If the primary verification is not passed, the EV certificate applicant is required to modify the material of domain name register and then apply for EV Certificate.

4. The RA reviewer verifies whether the legal domain name holder is identical with the certificate holder (whois function is also used), examine whether material is true, make comparison on the application information in RA system and meanwhile make confirmation with the manager and operator by phone.

(Note: In terms of high-risk applicants (such as financials), other than marked for high-risk or suspicious certificate application by CA, additional precautions are needed, which including an inspection of the organization name, see if there is a targeted phishing and other fraudulent behavior.)

5. If the confirmation is passed, the RA reviewer will log on RA system, approve the certificate application and send the first 13 bits of Reference No. and Authorization Code by email and the last 13 bits by phone to the operator of certificate application. If the conformation fails to be passed, the EV Certificate application is rejected; all materials will be returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply.

6. When the application letter is submitted to legal processing authority delegated by Trusted Network Service Center, there must be certificate for attest issued onsite by authority personnel and such attested personnel shall sign on the certificate.

4.1.2 Multiple domain name EV Certificate

1. The application operator for EV Certificate submits application materials to the data processor of LRA.

- Identity certification of EV certificate applicant:
  - Provided by enterprise: duplicate copy of Organization Code Certificate or Enterprise Business License for Enterprise's Legal Person (with each page sealed);
  - Provided by government authority: duplicate copy of Organization Code Certificate (with each page sealed);
  - Provided by institution: duplicate copy of Organization Code Certificate (with each page sealed);
  - Provided by social club: duplicate copy of Organization Code Certificate (with each page sealed);
  - Account opening certificate issued by bank (with each page sealed).
- Original copy of application letter for EV certificate registration (with each page sealed).
- When the EV certificate applicant is enterprise/government authority/institution/social group, the duplicate copies of identity certificates for manager and operator need to be submitted.

2. The data processor for LRA carries out primary verification. It obtains, through domain name registration inquiry (whois) function, the material for domain name register material of applied EV certificate, check whether the domain name register is identical with the applicant of EV Certificate and determine whether the EV Certificate register actually owns such domain name through primary verification.

3. After the primary verification of data processor of LRA is passed, input the above material through RA system; submit the application and all the paper application material to the RA reviewer of CNNIC RA. If the primary verification is not passed, or the EV Certificate and domain name register are not identical, the EV certificate applicant is required to modify the material of domain name register and then the hosted authority applies for multiple domain name certificate, or delete domain names that are not in conformity with material in the

multiple domain name certificate.

4. The RA reviewer verifies whether the legal domain name holder is identical with the certificate holder (whois function is also used), examine whether material is true, make comparison on the application information in RA system and meanwhile make confirmation with the manager and operator by phone.

5. If the confirmation is passed, the RA reviewer will log on RA system, approve the certificate application and send the first 13 bits of Reference No. and Authorization Code by email and the last 13 bits by phone to the operator of certificate application. If the conformation fails to be passed, the EV Certificate renewal is rejected; all materials will be returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply for renewal.

6. When the application letter is submitted to legal processing authority delegated by Trusted Network Service Center, there must be certificate for attest issued onsite by authority personnel and such attested personnel shall sign on the certificate.

4.1.3 Methods for application

The managers responsible for the application of EV Certificate must submit an application in the LRA of CNNIC Trusted Network Service Center designated by CNNIC. CNNIC Trusted Network Service Center (including RA) does not accept application directly oriented for the applicant.

The EV Certificate applicant may download the applicant letter or user agreement directly from the official website of CNNIC. The Certificate Signing Request (CSR) needs to be directly submitted online.

4.2 Renewal of EV Certificate

Before the expiration of Certificate for EV Certificate holder, the holder needs to obtain a new EV Certificate so to keep the continuity of certificate use. The holder generates another new key pair to replace the outdated key pair, which is called “key update’. However, in

some cases, the certificate holder wishes to apply for a certificate for the existing key pair, which is called “certificate update”.

In the certificate system of CNNIC Trusted Network Service Center, Certificate Signing Request needs to be regenerated by Certificate holder for EV Certificate renewal. Meanwhile, CNNIC Trusted Network Service Center requests certificate users to use the key pair that differs from the original one for application and the old Certificate Signing Request shall not be allowed to use (or “key update” is compulsory).

The renewal period of EV Certificate is within three months prior to the expiration of the current certificate. CNNIC Trusted Service Center will refuse renewal application in other terms.

After renewal, the new EV Certificate shall be immediately installed after being downloaded.

The extension of renewal terms: expiration period of new certificate=current time+ time length of newly purchased EV Certificate +time length left for the current EV Certificate.

4.2.1 Single domain name EV Certificate renewal

1. The manager responsible for EV Certificate application submits the application material to the data processor of LRA:

- Identity certification of EV certificate applicant:
  - Provided by enterprise: duplicate copy of Organization Code Certificate or Enterprise Business License for Enterprise's Legal Person (with each page sealed);
  - Provided by government authority: duplicate copy of Organization Code Certificate (with each page sealed);
  - Provided by institution: duplicate copy of Organization Code Certificate (with each page sealed);
  - Provided by social club: duplicate copy of Organization Code Certificate (with each page sealed);
  - Account opening certificate issued by bank (with each page sealed).
- Original copy of application letter for EV certificate registration (with each page sealed).

- When the EV Certificate applicant is an enterprise/government authority/institution/social club, it also needs to submit duplicate copies of the identity certification of manager and operator.

2. The data processor of LRA inputs the above material through RA system and submits the application.

3. The data processor of LA submits all application material, in a safe manner, to the RA reviewer of CNNIC RA.

4. The RA reviewer verifies material and makes comparison on the application information and the original registration information in the domain name certificate, meanwhile confirm with the operator and manager by phone.

5. If the confirmation is passed, the RA reviewer will log on RA system, approve the certificate application and send the first 13 bits of Reference No. and Authorization Code by email and the last 13 bits by phone to the operator of certificate application. If the conformation fails to be passed, the EV Certificate renewal is rejected; all materials will be returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply for renewal.

6. The operator for EV Certificate application will generate Certificate Signing Request (CSR) in the Web Server.

7. The operator for EV Certificate application access CNNIC Certificate downloading page, submit CSR and input Reference No. and Authorization Code.

8. CNNIC Trusted Network Service Center issues EV Certificate and the operator for EV Certificate application is responsible for installation.

4.2.2 Multiple domain name EV Certificate renewal

1. The operator for EV certificate application submits the application material to the data processor of LRA.

- Identity certification of EV certificate applicant:
  - Provided by enterprise: duplicate copy of Organization Code Certificate or

Enterprise Business License for Enterprise's Legal Person (with each page sealed);

- Provided by government authority: duplicate copy of Organization Code Certificate (with each page sealed);
- Provided by institution: duplicate copy of Organization Code Certificate (with each page sealed);
- Provided by social club: duplicate copy of Organization Code Certificate (with each page sealed);
- Account opening certificate issued by bank (with each page sealed).

- Original copy of application letter for EV certificate renewal (with each page sealed).
- When the EV Certificate applicant is an enterprise/government authority/institution/social club, it also needs to submit a duplicate copy of the identity certification of managers and operators.

2. The data processor of LRA inputs the above material through RA system and submits the application.

3. The data processor of LA submits all application material, in a safe manner, to the RA reviewer of CNNIC RA.

4. The RA reviewer verifies material and makes comparison on the application information and the original registration information in the domain name certificate, meanwhile confirm with the operator and manager by phone.

5. If the confirmation is passed, the RA reviewer will log on RA system, approve the certificate application and send the first 13 bits of Reference No. and Authorization Code by email and the last 13 bits by phone to the operator of certificate application. If the conformation fails to be passed, the EV Certificate renewal is rejected; all materials will be returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply for renewal.

6. The operator for EV Certificate application will generate Certificate Signing Request (CSR) in the Web Server.

7. The operator for EV Certificate application access CNNIC Certificate downloading page,

submit CSR and input Reference No. and Authorization Code.

8. CNNIC Trusted Network Service Center issues EV Certificate and the operator for EV Certificate application is responsible for installation.

4.3 Reissuing of EV Certificate

In the EV Certificate system of CNNIC Trusted Network Service Center, Certificate Signing Request (CSR) is needed for the issuing of EV Certificate. Meanwhile, CNNIC Trusted Network Service Center requests to use key that differs from the original key for application and the old certificate request document is not allowed to use.

After the reissuing of new certificate, the original EV Certificate shall be immediately nullified and the period of validity for new EV Certificate shall be the same with the original certificate.

4.3.1 Single domain name certificate reissuing

1. The operator for EV Certificate application submits the application material to the data processor of LRA:

- Original copy of application letter of EV Certificate reissuing (sealed)
- Duplicate copy of identity certification for operator of authorized organization.

2. The data processor of LRA inputs the above material through RA system and submits the application.

3. The data processor of LA submits all application material, in a safe manner, to the RA reviewer of CNNIC RA.

4. The RA reviewer verifies material and makes comparison on the application information and the original registration information in the domain name certificate, meanwhile confirm with the operator and manager by phone.

5. If the confirmation is passed, the RA reviewer will log on RA system, approve the certificate application and send the first 13 bits of Reference No. and Authorization Code by email and the last 13 bits by phone to the operator of certificate application. If the conformation fails to be passed, the EV Certificate reissuing is rejected; all materials will be

returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply for reissuing.

6. The operator for EV Certificate application will generate Certificate Signing Request (CSR) in the Web Server.

7. The operator for EV Certificate application access CNNIC Certificate downloading page, submit CSR and input Reference No. and Authorization Code.

8. CNNIC Trusted Network Service Center issues EV Certificate and the operator for EV Certificate application is responsible for installation.

4.3.2 Multiple domain name certificate reissuing

1. The operator for EV Certificate application submits the application material to the data processor of LRA:

- Original copy of application letter for EV certificate issuing (with each page sealed)
- Submit the duplicate copy of valid personal identity certification when the EV Certificate applicant is a natural person and duplicate copy of identity certification of unit operator and manager when the applicant is an enterprise/government authority/institution/social club.

2. The data processor of LRA inputs the above material through RA system and submits the application.

3. The data processor of LRA submits all application material, in a safe manner, to the RA reviewer of CNNIC RA.

4. The RA reviewer verifies material and makes comparison on the application information and the original registration information in the domain name certificate, meanwhile confirm with the manager (if any) by phone.

5. If the confirmation is passed, the RA reviewer will log on RA system, approve the certificate application and send the first 13 bits of Reference No. and Authorization Code by email and the last 13 bits by phone to the operator of certificate application. If the conformation fails to be passed, the EV Certificate reissuing is rejected; all materials will be

returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply for reissuing.

6. The operator for EV Certificate application will generate Certificate Signing Request (CSR) in the Web Server.

7. The operator for EV Certificate application access CNNIC Certificate downloading page, submit CSR and input Reference No. and Authorization Code.

8. CNNIC Trusted Network Service Center issues EV Certificate and the operator for EV Certificate application is responsible for installation.

4.4 Alternation of EV Certificate

4.4.1 Alternation of domain name for multiple domain name EV Certificate

The domain name alternation services are provided for multiple domain name EV certificate and domain names can be added, deleted and modified.

1. The operator for EV Certificate application submits its application material to the data processor of LRA:

- Original copy of domain name alternation for EV Certificate (with each page sealed)
- Identity certification for certificate applicant
  - Provided by enterprise: duplicate copy of Organization Code Certificate or Enterprise Business License for Enterprise's Legal Person (with each page sealed);
  - Provided by government authority: duplicate copy of Organization Code Certificate (with each page sealed);
  - Provided by institution: duplicate copy of Organization Code Certificate (with each page sealed);
  - Provided by social club: duplicate copy of Organization Code Certificate (with each page sealed);
  - Account opening certificate issued by bank (with each page sealed). Original copy of application letter for EV Certificate renewal.

- When the EV Certificate applicant is an enterprise/government authority/ institution/social club, it also needs to submit a duplicate copy of the identity certification of managers and operators.

2. The data processor of LRA inputs the above material through RA system and submits the application.

3. The data processor of LA submits all application material, in a safe manner, to the RA reviewer of CNNIC RA.

4. The RA reviewer verifies material and makes comparison on the application information and the original registration information in the domain name certificate, meanwhile confirm with the manager (if any) by phone.

5. If the confirmation is passed, the RA reviewer will log on RA system, approve the certificate application and send the first 13 bits of Reference No. and Authorization Code by email and the last 13 bits by phone to the operator of certificate application. If the conformation fails to be passed, the EV Certificate renewal is rejected; all materials will be returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply for renewal.

6. The operator for EV Certificate application will generate Certificate Signing Request (CSR) in the Web Server.

7. The operator for EV Certificate application access CNNIC Certificate downloading page, submit CSR and input Reference No. and Authorization Code.

8. CNNIC Trusted Network Service Center issues EV Certificate and the operator for EV Certificate application is responsible for installation.

* Note: After the alternation of domain name, the original EV Certificate must be immediately nullified. After new EV Certificate is downloaded, it must be immediately installed and the period of validity for EV Certificate shall be the same with the original certificate.

4.5 Audit of EV Certificate

Where the EV Certificate applied by user is more than one year old, annual inspection

needs to be made and the specific operations shall be the same with the submitted material in its application.

4.6 EV Certificate Verification Process

CNNIC Trusted Network Service Center completely conforms to *EV guideline* and makes strict verification on the information contained in the certificate before its issuance of EV Certificate. The major verification process and measures are as follows:

4.6.1 Verification on legal existence and identity of applicant

1) Verification requirements

EV Certificate shall be oriented for enterprise, institution and organizational club, etc. instead of individual.

- It must ensure the existence of the applicant;
- The entity name and EV Certificate applicant name shall be identical
- Registration No. allocated by governing region for establishment or registration or date of establishment if Registration No. is not available.
- Identity and address of Registration Authority

2) Verification methods

- Verification on application unit entity

The applicant needs to submit the following material:

Enterprise legal person: duplicate copy of Organization Code Certificate or Enterprise Business License for Enterprise's Legal Person;

Institution: duplicate copy of Organization Code Certificate;

Government authority: duplicate copy of Organization Code Certificate;

Social club: duplicate copy of Organization Code Certificate.

The reviewer of CNNIC Trusted Network Service Center will make comparison between the basic information as contained in the identity certification document provided by the

applicant (including company name, form of construction, Registration No., legal person, registered capital, data of establishment, annual inspection) and basic information of the applicant provided by the third party so to confirm whether the identity certification documents of such applicant is true.

- Verification on major individual

1) Face-to-face verification: The filling and signature of *Application Letter of CNNIC EV Certificate* in the User Agreement must be verified face to face by the personnel of registrar of CNNIC Trusted Network Service Center. In addition, the registrar of CNNIC Trusted Network Service Center also needs to collect materials, including identity certification of operator and manager, two copies of written certification and other application materials according to need.

2) One of the two copies of written certification shall be from financial institution such as:

- Valid credit card
- Valid debit card
- Bank statement within six months from financial institution
- Mortgage statement within six months from recognized borrower
- Duplicate copy of account opening certificate issued by bank

Other documents include:

- Fixed telephone bill
- Birth Certificate
- Tax bill from local authority in the current year

3) The identity certificates of manager and operator provided by the applicant; the reviewer of CNNIC Trusted Network Service Center will make verification through the identity access platform of Ministry of Public Security of the People's Republic of China.

4.6.2 Pseudonym or false name of applicant

The applicant shall not use pseudonym or false name to apply for certificate and in the certificate.

4.6.3 Verification on physical operation address and contact telephone

In order to verify the physical existence of the application unit, CNNIC Trusted Network Service Center must ensure that the physical address provided by the applicant is the business address of the application unit or its subsidiary or parent company and the telephone number provided by the applicant shall be the one of business address.

The reviewer of CNNIC Trusted Network Service Center will carry out certification on physical operation address and telephone through telecommunication operation website or by way of telephone and email.

4.6.4 Verification on existence of applicant operation

If the period for the establishment of application unit is not more than three years, CNNIC Trusted Network Service Center must confirm its business ability.

- CNNIC Trusted Network Service Center will directly obtain certification documents from financial institution and has confirmed that the applicant holds demand deposit in such institution; or
- The application unit needs to submit the Attorney Opinion Letter or Accounting Letter with demand deposit in the financial institution.

4.6.5 Verification on domain names of applicant

In order to verify that the applicant has the sole right to manage the listed domain names, CNNIC Trusted Network Service Center checks whether the domain name owner and the application unit are identical through WHOIS inquiry.

If the domain name owner and the application unit are not identical, the applicant needs to add:

- Authorization and identity certification of domain name holder or seal the authorized unit;
- Relevant description material and registration contract of domain name.

4.6.6 Verification on name, title and authority of manager and operator

The EV Certificate application of CNNIC Trusted Network Service Center has the following roles:

- Operator: The one who trusts server shall be the employee o authorized organization and the independent host shall be the employee of application unit.
- Manager: The manager of legal entity shall be the authorized delegate of legal representative and the manager of non-legal entity shall be the responsible person or its authorized delegate. Such person shall be the direct manager of operator.
- Contract signer: operator and manager.
  - The reviewer of CNNIC Trusted Network Service Center will make official verification on the identity cards of manager and operator;
  - In addition, the reviewer will make confirmation, by phone, on the information like title with manager, operator, workers of reception desk (telephone exchange) or personnel from Human Resources or other staff members.
  - Applicant Representative: In the case where CA and Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the applicant, employed by the applicant, or an authorized agent who has express authority to represent the applicant , and who has authority on behalf of the applicant to acknowledge and agree to Terms of Use.

4.6.7 Verification on certificate request and user agreement

The EV Certificate request of EV Trusted Network Service Center includes application letter and final user agreement, which needs to be signed by manager and operator. The reviewer of CNNIC Trusted Network Service Center will make confirmation by phone with manager and operator.

4.6.8 Other verification requirements

4.6.8.1 High-risk applicant

CNNIC Trusted Network Service Center will regular pay attention to and collect the list of Phishing Sites and make reference to the list of Phishing sites published by Anti-Phishing Working Group (APWG) and Anti-Phishing Alliance of China (APAC). It will control or reject strictly and carefully on the application of such website.

4.6.8.2 Rejected issuance list and other blacklists

For any organization or individual who is forbidden to pursue commercial activities by national or local governments, CNNIC Trusted Network Service Center will also forbid issuing EV Certificate to such users.

4.7 Termination of EV Certificate

CNNIC Trusted Network Service Center shall have the right to terminate its issued EV domain name certificate in case of the following conditions:

1. False information exists in the material provided when EV Certificate holder applies for domain name certificate after later examination;
2. The EV Certificate holder fails to fulfill the obligations as agreed in the Certificate Holder Agreement;
3. The EV Certificate holder requests the termination of domain name certificate;
4. The main body of EV Certificate holder dies out;
5. The EV Certificate holder alters the usage of domain name certificate;
6. Security damage on certificate key is found;
7. Other conditions as provided by law or regulation.

4.7.1 Procedures for termination request

When CNNIC Trusted Network Service Center has enough reason to believe the need to

terminate EV Certificate, the relevant personnel of CNNIC Trusted Network Service Center CA or RA may submit its request for the termination of EV Certificate through inner determined procedures. Upon the termination of EV Certificate, CNNIC Trusted Network Service Center will notify the EV Certificate holder about reasons for having been terminated or being terminated in an appropriate way including email and fax, etc.

The EV Certificate holder may also request to terminate its EV Certificate through terminate procedures. When the EV Certificate holder submits its request for termination, it also needs to provide materials in the provision of certificate application as the information for identity certification.

4.7.2 Certificate issue report and relevant mechanism

CNNIC has 7*24 hours certificate issue report and reception mechanism and may make investigation and determination on the certificate that has received report whether to cancel or adopt other proper actions within 24 hours after receiving the report. It mainly includes the process of recognition on the information below:

1. Recognition on nature of issue;
2. Investigation on issue reporting times;
3. Verification on the identity of reporter;
4. Conformity with relevant laws and regulations.

4.7.3 Duration for processing of termination request

The processing mechanism of 24*7 hours is available for the termination request of CNNIC Trusted Network Service Center Registration Authority (RA). It adopts the way of phone or email and will immediately deal with the process after receiving request for termination.

4.7.4 Termination of Single domain EV Certificate

1. The EV Certificate holder submits the paper request material for termination to the data processor of LRA.

For independent server, the application material shall include:

- Original copy of application letter for certificate termination (with each page sealed).
- Submit the duplicate copy of valid personal identity certification when the EV Certificate applicant is a natural person and duplicate copy of identity certification of unit operator and manager when the applicant is an enterprise/government authority/institution/social club.

For the hosted server, the application material shall include:

- Original copy of application letter for termination of EV Certificate (with each page sealed)
- Duplicate copy of identity certification for authorized organization operator.

2. The data processor of LRA inputs the above material through RA system and submits the application.

3. The data processor of LA submits all application material, in a safe manner, to the RA reviewer of CNNIC RA.

4. The RA reviewer verifies material and makes comparison on the application information and the original registration information in the domain name certificate, meanwhile confirm with the manager (if any) by phone.

5. If the confirmation is passed, the RA reviewer will directly terminate such domain name certificate. If the conformation fails to be passed, the EV Certificate termination is rejected; all materials will be returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply for termination.

4.7.5 Termination of multiple domain name EV Certificate

1. The EV Certificate holder submits the paper request material for termination to the data processor of LRA.

For independent server, the application material shall include:

- Original copy of application letter for certificate termination (with each page sealed).
- Submit the duplicate copy of valid personal identity certification when the EV Certificate applicant is a natural person and duplicate copy of identity certification of

unit operator and manager when the applicant is an enterprise/government authority/institution/social club.

For the trusted server, the application material shall include:

- Original copy of application letter for termination of EV Certificate (with each page sealed)
- Duplicate copy of identity certification for authorized organization operator.

2. The data processor of LRA inputs the above material through RA system and submits the application.

3. The data processor of LA submits all application material, in a safe manner, to the RA reviewer of CNNIC RA.

4. The RA reviewer verifies material and makes comparison on the application information and the original registration information in the domain name certificate, meanwhile confirm with the manager (if any) by phone.

5. If the confirmation is passed, the RA reviewer will directly terminate such domain name certificate. If the conformation fails to be passed, the EV Certificate termination is rejected; all materials will be returned to LRA and reasons for rejection will be added. LRA will communicate with the application operator, make relevant modification on rejection reasons and reapply for termination.

CNNIC Trusted Network Service Center will publish the termination status into the Certificate Revocation List, or terminate the usage effect of such EV Certificate.

4.8 Issuance and acceptation of EV Certificate

4.8.1 Issuance of single domain name EV Certificate

1. The operator for EV Certificate Application generates Certificate Signing Request in the Web server;

2. The operator of EV Certificate accesses the downloading page of CNNIC Certificate; submit CSR and input Reference No. and Authorization Code.

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

4. CNNIC Trusted Network Service Center issues EV Certificate and the operator for certificate application downloads and installs it.

5. The completion for EV Certificate issuance of CNNIC Trusted Network Service Center indicates that the applicant has accepted the services provided by the Center.

4.8.2 Issuance of multiple domain name EV Certificate

1. The operator for EV Certificate Application generates Certificate Signing Request in the Web server;

2. The operator of EV Certificate accesses the downloading page of CNNIC Certificate; submit CSR and input Reference No. and Authorization Code.

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

4. CNNIC Trusted Network Service Center issues EV Certificate and the operator for certificate application downloads and installs it.

5. The completion for EV Certificate issuance of CNNIC Trusted Network Service Center indicates that the applicant has accepted the services provided by the Center.

4.8.3 Certificate Issuance

The certificate issued by CNNIC Trusted Network Service Center is not stored in the storage pool for issuance; however, we can inquiry the registration information for EV Certificate through the website of CNNIC Trusted Network Service Center.

4.8.4 Forms of publication for terminated information

As for the terminated information in EV Certificate, except HTTP service provides CRL inquiry, CNNIC Trusted Service Center also provides OCSP inquiry.

4.9 Audit

After CNNIC Trusted Network Service Center has completed all verification and issuance of EV Certificate, the reviewer will make regular examination on all procedures and the

examination results will be recorded. Meanwhile, it will accept the regular audit work of audit authority formulated by CICA/AICPA.

5. Provisions about certificate issuance

This chapter mainly deals with the relevant legal requirements digital certificate of CNNIC Trusted Network Service Center.

5.1 Duties and Obligations of CNNIC Trusted Network Service Center

In accordance with regulations, CNNIC Trusted Network Service Center is a recognized certification authority, who issues, terminates certificate and makes use of open storage pool to issue Certificate Revocation List, etc. In accordance with this EV CPS, the Certification Authority of CNNIC Trusted Network Service Center has the following obligations:

b) Abide by this EV CPS, inner procedure, other relevant regulations and procedures;

c) Abide by local laws and regulations;

d) Receive the request of Registration Authority and timely issue EV certificate;

e) Ensure system security, including key generation and protection, etc.

f) Terminate certificate and issue timely EV Certificate Revocation List (EV CRL);

g) Issue notice immediately in case of key disclosure;

h) Strictly verify the request for EV certificate application;

i) Provide services for operations of EV certificate renewal, annual inspection and update, etc.

5.2 Exemption of responsibility for CNNIC Trusted Network Service Center

CNNIC Trusted Network Service Center will adopt proper technical and management measures, exercise its rights on all EV certificate holders and relying parties and fulfill its obligations. CNNIC Trusted Network Service Center does not guarantee the services provided in accordance with this EV CPS are uninterrupted or infallible.

That is to say, although CNNIC Trusted Network Service Center or RA on behalf of the

Center adopts appropriate technical and management measures in accordance with rights and obligations to be exercised by EV CPS, if the certificate holder or relying party suffers from debt, injury or damage of any nature from public key infrastructure or related, all EV certificate holders promise that CNNIC Trusted Network Service Center and RA will not compensate for any responsibility, loss or damage.

On the premise that CNNIC Trusted Network Service Center or RA on behalf of the Center has adopted appropriate technical and management measures, if the EV Certificate holder suffers from loss or injury due to trusting false or fake digital signature supported by EV Certificate, issued by CNNIC Trusted Network Service Center, of another EV Certificate holder, CNNIC Trusted Network Service Center or RA on behalf of it shall not be liable.

On the premise that CNNIC Trusted Network Service Center has adopted reasonable technical or management methods to prevent or ease the consequence of uncontrolled events, if EV Certificate holder suffers from serious impact due to the fact that CNNIC Trusted Service Center fails to control, CNNIC Trusted Network Service Center shall not be liable.

The situations beyond the control of CNNIC Trusted Network Service Center include but not limited to the unavailability of internet, telecommunications and other infrastructures, or natural disaster, war, military action, national emergency, disease, fire, flood, earthquake, strike, riot or omission or intentional behavior of other certificate holders or other third parties.

5.3 Duties and obligations of certificate holder

The certificate holder shall:

a) Complete application procedures appropriately and sign or confirm certificate holder agreement in the appropriate table; Fulfill obligations to be carried out in accordance with such agreement and ensure the accuracy of statement made in the application certificate;

b) Abide by procedures about completing certificate that are described in this EV CPS;

c) Promise to protect the confidentiality and completeness of private key of its certificate so to prevent loss, disclosure and utilization without authorization by proper prevention

measures;

d) Report to CNNIC Trusted Network Service Center, if the private key of its EV certificate is lost or disclosed, about such loss or disclosure;

e) Give a notice timely to CNNIC Trusted Network Service Center about any change of EV certificate holder materials;

f) Report to CNNIC Trusted Network Service Center if EV certificate needs to be terminated in case of Section 4.5.2, this EV CPS;

g) Make guarantee on CNNIC Trusted Network Service Center and show to all certificate relying parties that the facts described in the Section 5.5 below are true within the terms of certificate;

h) EV certificate shall not be used for exchange where it is well-known that CNNIC trusted Network Service Center may terminate EV certificate under this EV CPS, or EV certificate holder puts up with application for termination, or CNNIC Trusted Network Service Center proposes to terminate EV certificate under this EV CPS and notify the EV certificate holder;

i) Give a notice to the EV certificate relying party pursuing any exchange to be finished and explicitly explain that the EV certificate for exchange needs to be terminated (applied by CNNIC Trusted Network Service Center or EV certificate holder) and EV certificate relying party shall not trust such certificate in the exchange, where it is well-known that CNNIC trusted Network Service Center may terminate EV certificate under this EV CPS, or EV certificate holder puts up with application for termination, or CNNIC Trusted Network Service Center proposes to terminate EV certificate under this EV CPS and notify the EV certificate holder;

j) The use of EV certificate only limits to legal purposes and conformity with the relevant EV certificate policy and this EV CPS (or other published commercial matters). If the register has enough reason to believe that the correspondent private key and public key used by EV certificate have the risk of disclosure, report in time to CNNIC Trusted Network Service Center for the termination of EV certificate;

k) The EV certificate holder admits that if it fails to fulfill its obligations under the above clauses, it shall compensate for the damage or loss potentially caused to CNNIC Trusted Network Service Center or other relying parties.

5.4 Promise of certificate holder

The applicant shall sign or decide to accept an agreement (under the provisions of this EV CPS), wherein one article is recorded. The applicant promise under such article that once the applicant has accepted the certificate that is issued under this EV CPS, it means that it has made promise to CNNIC Trusted Network Service Center and statement on all other relevant personnel (especially relying parties) within the terms of certificate and the above facts will be kept true:

- None except EV certificate holder and its authorized persons has used the private key of EV certificate holder;
- Each digital signature generated by using the private key of certificate holder that relates to public key, contained in EV certificate of holder is actually the one of certificate holder;
- All materials contained in EV certificate and all statements made by certificate holder are true;
- EV certificate will only used for legal purposes in conformity with this EV CPS recognition;
- All materials provided in the process of EV certificate application will not infringe on the trademark, service sign, business number, company name or any intellectual property of any third party.

5.5 Duties and obligations of Registration Authority (RA), CNNIC Trusted Network Service Center

The RA system is responsible for the application and approval of EV certificate applicant and EV certificate management as well as transmission of EV certification application information to Certification Authority. RA shall fulfill the following obligations:

- Verify the accuracy and truth of information submitted by the applicant under this EV CPS; make the passed EV certificate application valid and transmit it to Certification Authority (RA). The EV certificate application includes certification registration,

reissuing, renewal, termination and multiple domain name modification, etc.

- Give a notice to the applicant about the approved or rejected EV certificate application
- Give a notice to EV certificate holder about the terminated EV certificate

There is only one registration authority in CNNIC Trusted Network Service Center, which is located in CNNIC.

CNNIC Trusted Network Service Center confirms the identity of LRA and authorizes LRA to perform the collection of materials registered by the certificate applicant. LRA has the obligations to collect the relevant information and make primary verification on the accuracy of such information when the certificate applicant performs certificate registration, reissuing, renewal, termination and multiple domain name modification.

5.6 Duties and obligations of relying party

The EV certificate relying party that trusts CNNIC Trusted Network Service Center shall:

- Trust the certificate only after EV certificate relying party has considered all factors and confirmed the actual rationality of the trusted certificate;
- Determine that the use of EV certificate is appropriate for the purposes under this EV CPS, or only EV certificate trusting CNNIC Trusted Network Service Center can be used for domain name certificate before trusting such EV certificate;
- Verify the certificate status on the EV Certificate Revocation List before trusting EV certificate;
- Execute all proper EV certificate route verification procedures;
- Indicate promise to accept the provisions of duty limitations regulated by this CPS.

5.7 Duties and obligations of repository, CNNIC Trusted Network Service Center

There is one repository in CNNIC Trusted Network Service Center, which includes EV Certificate Revocation List issued by the latest root and intermediate root, root certificate and intermediate root certificate of CNNIC Trusted Network Service Center, this EV CPS and one copy of CNNIC Trusted Network Service Center EV Certificate Policy and other relevant materials. The repository of CNNIC Trusted Network Service Center can be

accessed through the following URL:

http://www.cnnic.cn/index/0T/index.htm

The repository of CNNIC Trusted Network Service Center shall publish in time EV Certificate Revocation List and other information according to its formulated policy.

5.8 Notice to certificate duty limitation

CNNIC Trusted Network Service Center has given the following notice to certificate duty limitation on the issuance of certificate:

“The employees of CNNIC Trusted Network Service Center shall issue this EV certificate under the clauses as provided in EV Certificate Practice Statement that is issued by CNNIC Trusted Network Service Center, under the condition appropriate to this EV certificate and in accordance with relevant provisions”.

Therefore, any person shall read EV Certificate Practice Statement that is appropriate for EV certificate before it trusts this EV certificate (http://www.cnnic.cn/index/0T/index.htm).

The laws of the People’s Republic of China shall be applicable to this EV certificate. The relying party shall admit that any dispute or issue caused by trusting this EV certificate shall be governed by the laws of the People’s Republic of China.

If the relying party does not accept the terms and conditions for issuance of EV certificate, it shall not trust this EV certificate.

CNNIC Trusted Network Service Center issues this EV Certificate but does not need to carry on any responsibility or occupational duty.

The relying party shall ensure the trust action is fair and rational, without malice before it trusts this EV Certificate.

It shall ensure that the use of EV Certificate is actually proper for the purposes under EV CPS before it trusts this EV Certificate.

It shall check the status of this EV Certificate according to EV Certificate Revocation List and fulfill all proper route verification procedures of EV Certificate before it trusts this EV Certificate.

Although CNNIC Trusted Network Service Center has adopted reasonable technical and

management measure, if this EV Certificate is still inaccurate or misleading in any aspect, CNNIC Trusted Network Service Center shall not compensate for any loss or injury caused to the relying party.

If this EV Certificate is inaccurate or misleading in any aspect, while such inaccuracy and misleading is caused by the omission of CNNIC Trusted Network Service Center, CNNIC Trusted Network Service Center shall pay each relying party at most ten times of the purchase price of EV Certificate according to the testified loss caused by reasonably trusting inaccurate or misleading matters in this EV Certificate, except that such loss does not belong to and exclude: (1) any direct or indirect loss, including loss of profit or income, loss or injury of fame or commercial fame, business opportunity or chance, loss of item, loss or failure to use any data, device or software, etc.; (2) any indirect, correspondent and accidental loss or injury. Under such conditions, the trusted amount of EV Certificate shall be ten times of purchase price of EV Certificate in accordance with regulations.

If EV Certificate holder or relying party puts up with request on compensation to CNNIC, the reasons for such compensation shall relate to the issuance and termination of Certificate and they shall be raised within a half year (or earlier) since the certificate holder or relying party has been or should be aware of such matter. After the termination of the term for a half year, such request for compensation shall be abandoned and absolutely forbidden.

If this EV Certificate contains any intentional or reckless false statement made by CNNIC Trusted Network Service Center, this EV Certificate will not make any limitation to its legal responsibilities on the relying party who suffers from loss due to false statement in reasonably trusting this EV Certificate.

The legal responsibility limitations in this document shall not apply to the situations of personal injury or death (rarely occurring).

5.9 CNNIC Trusted Network Service Center’s Responsibility on EV Certificate with fault

If EV Certificate holder finds that the private or public key in the Certificate has faults, which causes the fact that it is unable to properly complete or almost impossible to complete the

exchange based on public key infrastructure upon its reception of EV Certificate, the Certificate holder shall immediately report such conditions to CNNIC Trusted Network Service Center s to terminate the EV Certificate and reissue a new one. Or if such conditions are found within three months of accepting EV Certificate and the certificate holder does not need EV Certificate, the holder may apply for refunding with the promise of CNNIC. If the EV Certificate holder reports to CNNIC about such faults after three months of accepting EV Certificate, the fees paid by it shall not be refunded.

5.10 Issuance of Certificate Revocation List

CNNIC Trusted Network Service Center shall preserve the right to issue Certificate Revocation List (CRL).

5.11 Information issuance

Important information will be updated gradually. Version No. and date of issuance shall be indicated in such update.

5.12 Information accuracy

The storage pool of CNNIC Trusted Network Service Center will keep 7*24 hours open in additional to at most four hours' regular and emergency maintenance so to ensure the accuracy and timeliness of its information.

5.13 Insurance plan

Once CNNIC Trusted Network Service Center violates *EV Certificate Holder Agreement* or any occupational duty, which causes injury or damage to EV Certificate holder or relying party, the legal responsibilities of CNNIC Trusted Network Service Center for any certificate holder or relying party only limits to the fact that each trusted certificate shall not exceed ten times of purchase price for EV Certificate.

If EV Certificate holder or relying party puts up with the request for compensation and the reasons for compensation have relation to the issuance and termination of EV Certificate,

such request shall be put up with within half a year (or earlier) prior to the certificate holder or relying party have been aware of such matter. After the termination of the term for a half year, such request for compensation shall be abandoned and absolutely forbidden.

Any responsibility due to deception or intentionally improper activities shall not be listed within the scope of this EV CPS, Certificate Holder Agreement, or EV Certificate issued by CNNIC Trusted Network Service Center or exceptions.

5.14 Provision collision

If collision exists between this EV CPS and Certificate Holder Agreement or other rules, directions and agreement, the certificate holder, relying party and CNNIC Trusted Network Center shall be bind by provisions of this EV CPS, unless these provisions are forbidden by law.

5.15 CNNIC Network Service Center’s Right to interpret

All materials in the Certificate issued under EV CPS shall be owned by CNNIC Trusted Network Service Center, including entity right, copyright and intellectual property in the relevant materials of this EV CPS,

5.16 Governing laws

This EV CPS shall be governed by the laws of the People’s Republic of China.

5.17 Legal authorities

If the dispute arising between parties can not be friendly resolved through consultation, it shall be submitted to China International Economic and Trade Arbitration Commission for arbitration. The decision to arbitration shall be final and binding to parties. The arbitration process shall be recorded in Chinese and be executed by courts with governing authority.

5.18 Severability

If any clause in this EV CPS is declared to be illegal, non-executable or invalid, any illegal statement thereof shall be deleted until such clauses become legal or executable and the original meaning of such clauses shall be kept. The non-executable nature of any clause in this EV CPS shall not injury the enforceability of other clauses.

CNNIC Trusted Network Service Center separates or combines the change of its operation range, manage and operation situations. Under such conditions, it will need to modify this EV CPS. The change of business activities shall be identical with the modification of EV CPS.

5.19 Fees

The registration, renewal, reissuing and domain name modification of multiple domain name certificate are charged and the cost depends on the regulations of market and administrative departments.

5.20 Refunding

CNNIC Trusted Network Service Center will not refund any trusted EV server certificate fees upon the issuance of certificate.