ITRUSCHINA™

CERTIFICATE

POLICY

V 1.4.2

Effective Date: Nov 1, 2020

Version Description:

iTrusChina Certificate Policy Version Control Table

Name & Version	Main Revision Description	Completion Time	Reviser
CP V1.3	1)Modified requirements for validation of IP address on section 3.2.2.5. 2) The CP first published in English	May 9, 2019	CP/CPS team
CP V1.4	1，According to the BR SC25, modified methods 3.2.2.4.2 in this CP as per the domain name validation methods 3.2.2.4.18 in BR. 2, Other revisions: adjust some format errors.	Apr 9, 2020	CP/CPS team
CP V1.4.1	Validity period of subscriber certificates and verification data are adjusted to 398 days.	May 20，2020	CP/CPS team
CP V1.4.2	1，Make corresponding adjustments According to the CAB Ballot SC28 and Ballot SC30， 2.，Other revisions: adjust some editing errors.	Nov 1, 2020	CP/CPS team

Contents

1. Introduction

1.1 Overview

1.1.1 Company Introduction

iTrusChina Co.,Ltd. (hereinafter referred to as "iTrusChina Digital Certification Authority", or "iTrusChina") is one of the first certification authorities which has obtained 'Electronic Authentication Service License' issued by Ministry of Industry and Information Technology. Since 2012, iTrusChina Digital Certification Service System has passed the security review organized by State Cryptography Administration. Since 2018, iTrusChina has started to implement the international security audit of WebTrust Services, plan to improve capacity of operational, management and services， and provide global electronic certification service for internet users with various needs on telecommunication and information security.

1.1.2 Certificate Policy (CP)

This *Certificate Policy* (CP for short) describes iTrusChina SSL certificate policy, which is a policy statement for iTrusChina SSL digital certificate service and applies to all SSL digital certificates issued and managed by iTrusChina and related participants. It formulates requirements and specifications in terms of service, law and technology for approving, issuing, managing, using, updating and revoking SSL certificates and related trusted services. These requirements and specifications include a complete set of single rule sets which are consistently applicable within iTrusChina to safeguard the security and integrity of iTrusChina SSL certificate service, hence the capability of providing trusted warranty within the framework of iTrusChina. This CP does not act as a lawful agreement between iTrusChina and related participants, as rights and obligations for iTrusChina and related participants depend on signed agreements therebetween.

This CP complies with the international standard of WebTrust and requirements of the latest versions of *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* ("Baseline Requirements", for short) and *Guidelines for the Issuance and Management of Extended Validation Certificates* ("EV Guidelines" , for short) *Network and Certificate System Security Requirements*（for short "NCSSR"）formulated by CA/Browser Forum. It also meets the structure and content requirements of *Public*

Encryption Key Infrastructure Certificate Policy and Certificate Business Structure of Internet X.509, i.e. RFC3647 Standard, and those of *GB 26855-2011-T Information Security Technology Public Key Infrastructure Policy and Certification Business Clarification Structure*, with appropriate adjustments made in accordance with China's laws and regulations as well as operational requirements of iTrusChina.

As an electronic certification authority (CA), iTrusChina generates root CA certificates and subordinate CA certificates under the constraints of this CP and issues subscriber certificates. Based on different types and application ranges, as the certificate holder, the subscriber can use the certificate for different purposes, such as website security protection, identity authentication, etc. Relying parties determine whether to trust a certificate or not according to the requirements on the obligations of relying parties specified in this CP. The CPS of iTrusChina is under the constraints of this CP and specifically describes how iTrusChina, a digital certification authority, provides certificates and related management, operation and safeguard measures. All certificate subscribers and relying parties of iTrusChina shall decide the use and trust on certificates in accordance with this CP and relevant regulations of CPS.

This CP is the supreme policy for SSL certificates of iTrusChina. In accordance with this CP, iTrusChina acts as an electronic certification authority and formulates CPS; in accordance with this CP and related CPS, RA identifies certificate service applications; in accordance with this CP and related CPS, subscribers, relying parties and other relevant entities determine the use and trust on certificates and fulfil relevant obligations.

1.2 Document Name and Identification

This document is called *iTrusChina Certificate Policy* ("iTrusChina CP" or this CP, for short), and CP is short for "Certificate Policy". In this document, CP is equivalent to the document name and applicable name as defined in this section.

The OID registered by iTrusChina is 1.2.156.112535, and meanwhile, iTrusChina will use policy identifiers as specified in Baseline Requirement. In this CP, iTrusChina assigns OIDs for each type of certificate as follows:

1) OID for EV SSL certificate policy: 1.2.156.112535.1.1.6.1；
2) OID for OV SSL certificate policy: 1.2.156.112535.1.1.5.1；
3) OID for DV SSL certificate policy: 1.2.156.112535.1.1.5.3。

iTrusChina also uses the policy object identifier reserved by CA/B Forum.

1) EV SSL Certificate Policy Object Identifier 2.23.140.1.1;

2) OV SSL Certificate Policy Object Identifier 2.23.140.1.2.2;

3) DV SSL Certificate Policy Object Identifier 2.23.140.1.2.1;

This CP has published an English version. In case of any inconsistency between the English version and the Chinese version, the Chinese version shall prevail.

1.3 PKI Participants

1.3.1 Certification Authorities (CA)

A certification authority (CA) refers to an entity authorized to issue digital certificates. iTrusChina is a third-party CA established by law in accordance with relevant provisions of *Electronic Signature Law of the People's Republic of China* and *Measures for the Administration of Electronic Certification Services*. iTrusChina has become a major participant of electronic certification service by issuing digital certificates, providing digital certificate authentication service to the parties engaged in electronic authentication activities.

1.3.2 Registration Authorities (RA)

A registration authority (RA) represents a CA to establish certificate registration process, confirm the identity of certificate applicants (subscribers), approve or reject certificate applications, approve subscribers' requests for certificate revocation or directly revoke certificates and approve subscribers' certificate renewal requests.

Besides acting as a CA, iTrusChina also act as an RA, and no external RA will be established separately.

1.3.3 Subscribers

Subscribers refer to who have applied and attained certificates from iTrusChina, being individuals, organizations or devices. A subscriber usually has to sign a contract with iTrusChina or RA to obtain a certificate and fulfils responsibilities as a certificate subscriber.

In digital signature applications, digital signers and certificate holders are equivalent to subscribers.

Subscriber represents the only entity bound with public keys in SSL certificates and possesses the ultimate control over the unique private key of the certificate. Subscriber uses SSL certificates within the scope of this CP and undertake obligations specified in this CP.

1.3.4 Relying Parties

A relying party of iTrusChina refers to an entity that uses and trusts the certificate issued by iTrusChina or its RA for an application. A relying party may or may not be a certificate subscriber of iTrusChina.

In order to trust or use a certificate, relying parties have to verify the revocation information of the certificate, including searching certificate revocation list (CRL) or searching certificate status via OCSP. Only after reasonable review can the relying party trust a certificate.

1.3.5 Other Participants

Other participants refer to other entities which provide related services for iTrusChina digital certification.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

SSL server certificates issued by iTrusChina are mainly used for identifying the identity of Website or Web server, proving the identity of Website and providing SSL encryption tunnels。

SSL server certificates issued by iTrusChina are classified as DV SSL (Domain Validation SSL) certificates, OV SSL (Organization Validation SSL）certificates and EV SSL (Extended Validation SSL）certificates. Subscribers can apply appropriate certificate types on their own according to actual needs.

1.4.2 Limited Certificate Uses

A SSL certificate issued by iTrusChina is functionally limited, only applicable to proper purposes matching the entity identity represented by the certificate.

Applications that go beyond the range of certificate uses defined in this CP are not protected by this CP.

1.4.3 Prohibited Certificate Uses

Certificates issued by iTrusChina are prohibited to be used under any circumstances in which the national laws and regulations be violated or national security be undermined, and is prohibited to be used for man-in-the-middle (MITM) or traffic management，otherwise the subscriber shall bear all the legal liability arising therefrom; meanwhile, all certificates are not designed to, intended to or authorized to be used in control equipment in dangerous environment or for the occasion where the failure is required to avoid, such as operations of nuclear equipment, navigation or telecommunication systems of space shuttles, air transportation control systems or weapon control systems, as any failure may lead to death, personal injury or severe environmental damage.

1.5 Policy Administration

1.5.1 Organization Administering the Policy Document

iTrusChina Security Policy Administration Committee (the Committee, for short) administer this CP, and the Committee is responsible for formulating, approving, releasing, implementing, updating and aborting this CP. iTrusChina Security Policy Administration Committee is formed by appropriate representatives from management team in iTrusChina, who are in charge of operation, R&D and HR department.

When more than half of the approval votes are cast by the Committee members, and only when the chairman of the Committee approves the approval, the CP version may be deemed to be approved.

The Operation Department of iTrusChina is responsible for daily work such as public consulting services concerning this CPS.

1.5.2 Contact Person

iTrusChina implements strict version control over Certificate policy and assigns a specific department responsible for related issues. For any question or suggestion, please contact us using the following methods:

If you need iTrusChina policy document, please send an email to itrus_cps@itrus.com.cn, or post to iTrusChina Co.,Ltd. The address is

Floor 4, Building 4, Courtyard 7, Shangdi Street 8, Haidian district, Beijing, PRC. 100085

Telephone Number: 0086-010-50947500

Fax Number: 0086-010-50947517/50947516

Official Website: https://www.itrus.com.cn

1.5.3 Person Determining CPS Suitability for the CP

iTrusChina Security Policy Administration Committee is the major organization for policy formulation and the supreme authority for the examination and approval of this CP to ensure the CPS conforms to this CP.

1.5.4 CP Approval Procedures

This CP is compiled by a team organized by iTrusChina Security Policy Administration Committee. After the compiling is completed, this team submits it to the Committee for verification. Upon approval of the Committee, this CP is officially published on the official website of iTrusChina.

This CP has been revised according to national laws and regulations, technical requirements, business development and the latest versions of Baseline Requirements, EV Guidelines and NCSSR published in CA/Browser Forum. The CP compiling team submits CP revised contents to iTrusChina Security Policy Administration Committee for examination. Upon approval of the Committee, the operation team will increment the version number, update publication time, effective time and revise record, and then officially publish the CP on iTrusChina official website. This CP will be updated and published at least once a year.

All officially published versions of this CP shall be put on record by Ministry of Industry and Information Technology within 30 days from the public publication date according to the regulations of *Measures for the Administration of Electronic Certification Services*.

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
Security Policy Administration	It refers to the supreme policy administration and supervision organization in the certification service system

Committee	and the decisive organization for CP consistency.
Certification Authority	It refers to a certificate authentication organization, and it is also an entity that issues certificates.
Registration Authority（RA）	It refers to an entity that is responsible for handling service requests from certificate applicants and certificate subscribers, submitting requests to certification authority, and creating the registration process for end certificate applicants. It is responsible for identifying and authenticating the identity of certificate applicants, initiating or delivering certificate revocation requests as well as approving the applications for updating certificates or keys on behalf of certification authority.
Certificate Policy (CP)	It refers to a set of named rule sets which are used to specify the applicability of certificates for a specific organization or applications with the same security needs. For example, a specific CP can specify that a type of certificate applies to the identification of products and services within the given price range for participants involved in business-to-business transactions.
Certification Practice Statement (CPS）	It refers to the statement of business practices adopted by Certification Authority for issuing, managing, revoking or updating certificates or keys.
Certification Path	It refers to a sequential certificate sequence (including the public key of the start object in the path), and the public key of the end object can be obtained by processing this sequence.
Policy Qualifier	It refers to information that depends on the policy and may exist in X.509 certificate together with CP identifier. The information may include available CPS, URL address of protocols of relying parties as well as texts of Terms of Use of certificates.

Digital Certificate	It refers to a digital signature certificate which used as a digital signature to identify the identity of the signer and the signer recognized the signature.
E-Signature	It refers to a technical means which has functions of identifying the identity of the signer and signifying that the signer accepts the signature data.
Digital Signature	It refers to a type of e-signature which uses an asymmetric cryptographic system to encrypt or decrypt the electronic record.
Electronic Signer	It refers to the one who holds the e-signature creation data and implements the e-signature in person or in the name of assigned representatives.
E-signature Relying Party	It refers to the one who trust e-signature certification certificates or e-signature and undertake related activities.
Private Key (E-signature creation data)	It refers to the data that is used in the process of electronic signing and reliably relates e-signature with electronic signer, such as characters, codes, etc.
Public Key (E-signature verifying data)	It refers to the data used by Subscriber to verify e-signature.
Subscriber	It refers to an entity that receives certificates from certification authority, namely certificate holder. In e-signature applications, Subscriber is the electronic signer.
Relying Party	It refers to an entity which relies on the authenticity of a certificate. In e-signature applications, it also refers to an e-signature relying party. A relying party may or may not be a subscriber.

1.6.2 Acronyms

Acronym	**Full Name**	**Chinese Translation**

CA	Certification Authority	电子认证服务机构，证书颁发机构
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
SSL	Secure Sockets Layer	加密套接层协议
CRL	Certificate Revocation List	证书撤消列表
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
OCSP	Online Certificate Status Protocol	在线证书状态协议
PIN	Personal Identification Number	个人身份识别码
PKCS	Public Key Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公共密钥基础设施
RA	Registration Authority	注册审核服务机构
RFC	Request For Comments	请求评注标准（一种互联网建议标准）

2. Publication and Repository Responsibility

2.1 Repositories

iTrusChina repository includes following contents: CP, CPS, Subscriber agreement, relying party agreement, Root CA certificate and all intermediate CA certificates.

2.2 Publication of Certification Information

iTrusChina publishes Repository on its official website https://www.itrus.com.cn/repository, and this website is the most important, timely and authoritative channel for iTrusChina to publish all the information.

iTrusChina provides Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) service so that Subscriber or Relying Party can check the status of the certificate in real time..

Besides, iTrusChina will also publish information using other possible ways as needed.

iTrusChina uses "itrus.com.cn" and "itrus.cn" as CAA query tags.

2.3 Time or Frequency of Publication

iTrusChina CP and CPS are available through Repository on a 24x7 basis.

iTrusChina publishes CP and CPS at least once a year.

iTrusChina will follow BR update of CA/B Forum regularly, and revise CP/CPS timely to perform compliance with BR standards.

Subscriber certificates issued by iTrusChina can be downloaded upon issuance, and Subscriber can obtain the issued certificate through certificate service sites, and check the certificate status via OCSP.

iTrusChina publishes CRL of subscriber certificates at least once in 96 hours and CRL of subordinate CA certificates at least once in 12 months; in case of revocation of subordinate CA certificates, iTrusChina will renew the CRL of CA certificate within 24 hours. In case of emergency, iTrusChina will independently decide the publication time and frequency of other contents in repositories, as such publication shall be timely, efficient and in compliance with national laws and regulations.

2.4 Access Controls on Repositories

The information in iTrusChina Repository is publicly available in read-only manner. Through network security protection, system security design and process management control iTrusChina will ensure that only authorized personnel can perform operations on repositories, such as add, delete, modify and publish the repositories.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Digital certificates issued by iTrusChina meet X.509 Standard, RFC 5280 standard and the requirements of CA/Browser Forum BR, and distinguished names assigned for certificate holders adopt the X.500 standard naming method. Regarding SSL server certificates issued by iTrusChina, all their domain names or IP addresses are added to Subject Alternative Name; meanwhile, a common name is a primary domain name or IP address, which should be a domain name or IP address that exists in Subject Alternative Name.

3.1.2 Need for Names to be Meaningful

Names included in subscriber certificates are symbolically meaningful, among which the subject identification name shall clearly identify the certificate holding organization and the network host server or internet domain name to be identified, and can be identified by relying parties. The subject identification name shall meet the requirements of relevant laws and regulations.

3.1.3 Anonymity or Pseudonymity of Subscribers

Subscribers of certificates mentioned in this CP shall not be anonymous or pseudo during certificate application.

3.1.4 Rules for Interpreting Various Name Forms

Digital certificates issued by iTrusChina conform to X.509 V3 Standard, and the format of distinguished names conforms to X.500 Standard.

3.1.5 Uniqueness of Names

In iTrusChina trust domain, certificates of different subscribers shall not share the same subject distinguished name, which must be unique. However, iTrusChina can use the unique subject distinguished name to issue multiple certificates for the same subscriber.

3.1.6 Recognition, Authentication and Role of Trademark

Certificates issued by iTrusChina does not contain any trademarks or other information which may infringe other parties' rights. iTrusChina don't validate trademark right or legal disputes when processing applications. iTrusChina has right to refuse applications and revoke any issued certificates when trademark disputes rise.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Certificate applicants shall prove the possession of the private key that corresponds to the public key to be registered, and the proving method is to include digital signature (PKCS#10) in the certificate application information.

3.2.2 Authentication and Domain Identity

3.2.2.1 Authentication of Organization Identity

The identity of any organization (including government organizations, enterprises and public organizations, etc.) that applies for various types of certificates (organization certificates, device certificates, etc.) shall be strictly authenticated, and authentication methods include:

Any material provided by the third party which can prove the actual existence of this organization, such as the legitimacy proof (Organization Code Certificate, business license, etc.) issued by governmental organizations as well as other proof materials provided by approved authority.

1. Confirm the authenticity of materials and information about the organization and whether the applicant has obtained sufficient authorization or other verification information or not via phone, mail, required proof documents or other similar methods.

2. Valid documents issued by governmental organizations on on-site interviews and on-site verifications performed by iTrusChina.

iTrusChina can use contents or correspondence in documents of the above-mentioned one to two items to verify the address of the organization and the authorized information of the applicant.

Use utility bills, bank statements, credit card statements, tax documents issued by the

government or other reliable forms of identification trusted by iTrusChina to verify subscriber’s address (not subscriber’s identity) and confirm the authenticity of the authorized application, i.e. the one who represents the organization for certificate application has been authorized. The confirming method can be power of the attorney of the organization and the identity material of the responsible person with the official seal affixed; or contact with the organization via phone, email, mail and other means obtained from the third party to confirm the identity of the applicant and the fact of authorized organization.

iTrusChina shall refer to the BR and EV Guidelines of the CA/B Forum to implement different methods of identity authentication based on different types of certificates applied by subscribers.

3.2.2.2 DBA/Tradename

Not applicable.

3.2.2.3 Verification of Country

If the country code is included in the subject of the certificate issued by iTrusChina, iTrusChina uses one or more of the following methods to verify:

a) Confirming the host country by checking the IP address displayed by the DNS record；

b) The ccTLD of the requested Domain Name;

c) Query government agencies or other trusted third-party data sources to confirm the country where the applicant's address is located through the methods in this CP 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

iTrusChina will verify the ownership of all domain names listed in a certificate, and will not delegate the performance of domain verification to a third party. For the verification of domain names, the verified entity can be a parent company, a subsidiary company or an affiliate company of the subscriber. iTrusChina shall confirm the domain name permission in the following ways:

3.2.2.4.1 Confirming the applicant’s control over the FQDN by sending a random value by email, SMS or postal mail and then receiving a confirming response utilizing the random value. The random value must be sent to an email address marked as domain name contact person or 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' followed by (' @ ')

and an authorized domain name, phone number, or email address. (as per the domain name verification methods in 3.2.2.4.2 and 3.2.2.4.4 in BR)

3.2.2.4.2 Confirming the subscriber’s control over the FQDN by modifying the agreed information under the directory of "/.well- known / pki-validation". (as per the domain name verification methods in 3.2.2.4.18 in BR)

3.2.2.4.3 Confirming the subscriber’s control over the domain name by checking whether the agreed random value exists in DNS CNAME, TXT or CAA records or not. Requirements: 1) authorized domain name; or 2) an authorized domain name with a prefix starting with underline character. (as per domain name verification & issuance in 3.2.2.4.7 in BR)

Note: The above-mentioned methods can be used to verify the control over FQDN, and CA can also issue certificates for other domain names with the same top-level domain name. This method is suitable for validating wildcard domain names.

3.2.2.5 Authentication for an IP Address

For all IP address listed in a certificate, iTrusChina should confirm the control over the IP by following methods:

3.2.2.5.1 Confirming the Applicant's control over the requested IP Address by modifying the agreed information in the "/.well-known/pki-validation" directory (according to the IP authentication method in 3.2.2.5.1 of BR).1. Checking the following links of Iana's official website to confirm that the IP address is not marked as Reserved IP.

3.2.2.5.2 Confirming the Applicant's control over the IP Address by sending a Random Value via email, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, SMS number, or postal mail address identified as an IP Address Contact(according to the IP authentication method in 3.2.2.5.2 of BR).

3.2.2.5.3 Confirming the Applicant’s control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under BR Section 3.2.2.4 (according to the IP authentication method in 3.2.2.5.3 of BR).

3.2.2.5.4 Confirming the Applicant's control over the IP Address by calling the IP Address Contact’s phone number and obtaining a response confirming the Applicant's

request for validation of the IP Address (according to the IP authentication method in 3.2.2.5.5 of BR).

3.2.2.5.5 Confirming the Applicant's control over the IP Address by performing the procedure documented for an “http-01” challenge in draft 04 of “ACME IP Identifier Validation Extension,” available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4 (according to the IP authentication method in 3.2.2.5.6 of BR).

3.2.2.5.6 Confirming the Applicant's control over the IP Address by performing the procedure documented for a “tls-alpn-01” challenge in draft 04 of “ACME IP Identifier Validation Extension,” available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4 (according to the IP authentication method in 3.2.2.5.7 of BR).

3.2.2.5.7 iTrusChina does not issue DV and EV certificates for IP addresses..

3.2.2.6 Wildcard Domain Validation

Regarding a wildcard domain name, iTrusChina verifies the domain name on the right side of the wildcard to ensure that the domain name is clearly owned by a business entity, social organization or government agency, etc. and is obtained through legal registration.

iTrusChina rejects certificate applications of the domain name on the right side of the wildcard being a top-level domain name, a common suffix or a domain name controlled by a domain name registration and administration organization, unless the subscriber can prove its rightful control of the entire domain namespace.

If necessary, iTrusChina needs to adopt other independent authentication methods to confirm the ownership of a domain name. If the subscriber’s assistance is needed, the subscriber cannot refuse such a request for any reason.

3.2.2.7 Data Source And Accuracy

3.2.2.7.1 Authentication data source

iTrusChina publicly discloses the source of the authentication data (Incorporating Agency /Registration Agency, etc.) on the official website. If necessary, please visit https://www.itrus.com.cn/repository.

iTrusChina will update and disclose in this document before using the new authentication data source.

3.2.2.7.2 Data source accuracy

Prior to using any data source as a reliable data source, iTrusChina shall evaluate the source for its reliability, accuracy and resistance for alteration or falsification, comply with CAB Forum BR section 3.2.2.7 and EV Guidelines section 11.11 for data source requirements, considering the following factors:

1. The age of the information provided;
2. The frequency of updates to the information source;
3. The data provider and purpose of data collection;
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering data.

iTrusChina shall obtain data from authoritative third-party data providers and carry out the authentication work as described in Section 3.2.

3.2.2.8 Certification Authority Authorization (CAA) Records

Prior to issuing a publicly trusted SSL certificate, iTrusChina shall check CAA records for each dNSName in the extension of the Subject Alternative Name of the certificate. iTrusChina will issue the certificate to subscriber within 8 hours after checking the CAA record. iTrusChina shall check the CAA record again if it exceeds 8 hours.

iTrusChina handles the property tags of "issue", "issuewild" and "iodef" in accordance with the regulations of RFC8659. If "itrus.com.cn" and “itrus.cn” are not contained in "issue" and "issuewild" tags, iTrusChina will not issue the corresponding certificate; if the tag "iodef" exists in CAA records, iTrusChina will determine whether to issue the certificate after communicating with the applicant.

iTrusChina treats a record lookup failure as permission to issue if:

1) the failure is outside the iTrusChina’s infrastructure;
2) the lookup has been retried at least once; and
3) the domain’s zone does not have a DNSSEC verification chain to the ICANN root.

3.2.3 Authentication of Individual Identity

For any person who applies for an identity certificate or an email certificate, iTrusChina shall verify the authenticity of the certificate application by verifying the subscriber's name and address, etc. The authentication methods include:

1. The subscriber should submit a legible copy of at least one currently valid identity certificate issued by the government (passport, driver's license, national ID card or equivalent certificates) for iTrusChina to verify the applicant's name.

2. iTrusChina verifies the authenticity of information such as identity materials, etc. by face-to-face audit or by telephone, post, etc.

3. Regarding an application in the name of an individual in an organization, proof materials provided by the organization shall also be submitted.

4. iTrusChina can also verify the personal identity of a subscriber through information obtained from a third party. If iTrusChina cannot get all the necessary information from a third party, it can entrust a third party for investigation or request the applicant to provide extra information and proof materials.

5. Regarding an application that is made by an entrusted person, a written proof document that proves the full authorization shall be submitted.

6. Regarding a certificate application in which a domain name, a device name or an email address is used as the certificate subject content, iTrusChina shall verify whether the individual applicant has the right or not, for example, asking the applicant to submit the domain name ownership document, ownership proof document or the applicant's written commitment to the ownership, etc.

iTrusChina also defines other authentication methods and materials required according to the authentication of individual identity of customers.

3.2.4 Non-verified Subscriber Information

In general, apart from the identity information required to be verified clearly and reliably for the type of a certificate, iTrusChina does not promise the authenticity of the subscriber's information that is not required to be verified and bears no legal responsibility.

3.2.5 Validation of Authority

If the applicant for a certificate containing subject identity information is an organization, iTrusChina shall verify the reliability of the communication information using the sources listed in 3.2.2.1, and use this information to confirm the authenticity of the certificate application with the subscriber representative or the authoritative source within the subscriber's organization (including but not limited to subscriber's main business offices, corporate offices and human resources offices).

If a subscriber specifies, in writing, the individuals who may request a certificate, iTrusChina will not accept any certificate requests that are outside this specification. iTrusChina may request the subscriber to provide a written letter of authorization verified and sealed by it.

3.2.6 Criteria for Interoperation

iTrusChina can interoperate with other certification authorities and require that their CPSs shall conform to the requirements of iTrusChina's CP and these authorities shall sign relevant agreements with iTrusChina.

If national laws and regulations have requirements over the matter, iTrusChina will strictly abide by them.

By now, iTrusChina has not issued any cross-certification certificate.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

iTrusChina support certificate subscribers' requests for re-key within the period of validity. Subscribers can choose to generate a new key pair to replace the one in use or about to expire.

After receiving a re-key request, iTrusChina will create a new certificate using the new request submitted by the subscriber. The new certificate will have the same subject information and the same period of validity as the old certificate.

3.3.2 Identification and Authentication of Re-key After Revocation

iTrusChina will not re-key when certificates are revoked.

3.4 Identification and Authentication for Revocation Request

Among iTrusChina's certificate practices, certificate revocation requests may come from subscribers or iTrusChina and RAs. In addition, if iTrusChina deems it necessary (see the relevant circumstance described in 4.9.1.1 of this CP), iTrusChina has the right to initiate revocation of subscribers' certificates.

After a subscriber submits a request to iTrusChina via email, fax, and telephone, etc., iTrusChina will contact the subscriber through the communication way that corresponds to

the certificate warranty level to confirm the person or organization that initiated the revocation request is indeed the subscriber or its authorizer. Depending on different environments, one or more of the following communication methods can be adopted: telephone, fax, email, mail or express service.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate application entities include individuals, organizations or entities.

4.1.2 Enrolment Process and Responsibilities

The SSL certificate registration operation complies with the guidelines issued by CA/Browser Forum through www.cabforum.org.

The applicant shall learn matters stipulated in subscriber agreements, this CP and the corresponding CPS, etc beforehand, especially contents related to range of application, rights, obligations and warranties of certificates.

The applicant shall submit the SSL certificate application form and relevant supporting documents to iTrusChina, which means that the applicant has already understood and accepted the above contents.

Subscribers shall generate key pairs by themselves, generate PKCS#10 certificate request file, submit to iTrusChina and pay any applicable fee.

Subscriber is responsible for providing true, complete and accurate certificate application information and materials to iTrusChina.

iTrusChina is responsible for checking the consistency between the certificate application information and identity proof documents provided by subscribers, and meanwhile, iTrusChina is responsible for the corresponding authentication.

According to *Electronic Signature Law of the People's Republic of China*, in the case that the applicant fails to provide true, complete and accurate information to iTrusChina or has any other fault which brings losses to e-signature relying parties and iTrusChina, the applicant shall undertake the corresponding legal and indemnification liability.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

After iTrusChina and its RA receive a subscriber's certificate application, iTrusChina shall identify and authenticate the subscriber’s identity in accordance with the requirements in Section 3.2 of this CP.

Based on prior rejected certificate requests or revoked certificates due to suspicion of phishing or other fraud purpose or other concerns, iTrusChina establishes and maintains a list of SSL certificate high-risk database, which will be queried when iTrusChina accepts a certificate application. For subscribers that exist in the list, iTrusChina will perform additional validation.

iTrusChina will perform a CAA record check for each dNSName in the certificate extension Subject Alternative Name, and determine whether to approve the certificate application according to the inspection method and result in 3.2.2.8.

After verifying application materials submitted by an applicant, based on the verification result, iTrusChina will decide whether to accept or reject the application or require the applicant to submit additional relevant materials. In the process of handling a certificate application, iTrusChina will ensure the consistency between certificate information and correct application information through effective means and issue the certificate to the right applicant.

Before the issuance of a certificate, if the data or proof documents obtained by iTrusChina from the sources specified in Section 3.2 of this CP are not more than 398 days old and the information has not changed, iTrusChina can use the data or proof documents to verify the information in OV and EV certificates. For DV certificates, iTrusChina does not reuse authentication data.

4.2.2 Approval or Rejection of Certificate Applications

iTrusChina should approve or reject an application based on authentication. If an application is rejected, iTrusChina shall notify the SSL certificate applicant in a proper manner within a reasonable time.

4.2.2.1 Approval of Certificate Applications

The registration authority (RA) may approve a certificate application if:

1) this application fully meets the regulations about identification and authentication of subscriber identity in Section 3.2 of this CP;

2) the applicant accepts or does not oppose the contents or requirements of subscriber agreements;

3) the applicant has paid the corresponding fees according to regulations.

4.2.2.2 Rejection of Certificate Applications

iTrusChina will reject a certificate application if:

1) this application does not meet the regulations about identification and authentication of subscriber identity in Section 3.2 of this CP;

2) the applicant cannot provide necessary identity proof materials;

3) the applicant opposes or cannot accept the relevant contents or requirements of subscriber agreements;

4) the applicant fails to or cannot pay corresponding fees according to regulations;

5) the certificate to be applied for contains a new gTLD (top-level domain name) under the consideration of ICANN (The Internet Corporation for Assigned Names and Numbers);

6) iTrusChina or the RA believes that the approval of this application will bring disputes, legal disputes or losses to iTrusChina.

Regarding rejected certificate applications, iTrusChina will inform the applicant of the failure of the application.

4.2.3 Time to Process Certificate Applications

The Certification Practice Statement (CPS) of iTrusChina shall stipulate a reasonable processing time of certificate applications, within which iTrusChina shall process the certificate application, whether to approve or reject it.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

When the root CA of iTrusChina signing the certificate, it is required a trusted internal role authorized by iTrusChina to directly conduct the certificate signing after strict approval process..

Before issuing a subscriber certificate, iTrusChina shall ensure that the RA has verified the authenticity of the received certificate application.

When a CA is used for certificate issuance, the RA packages the certificate request information into packets, and after signing and encrypting the packets, it sends them to the CA. The CA authenticates the integrity of the packet by verifying the signature on the packet and identifies the sender's identity and permissions based on the signer's information. After the authentication is passed, the CA will use the private key to sign the certificate request to generate a subscriber certificate.

4.3.2 Notification of Certificate Issuance to Subscribers

After the certificate issuance system of iTrusChina has issued a certificate, iTrusChina CA or RA shall notify the subscriber of the certificate issuance and provide subscribers with methods to obtain the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

iTrusChina believes that a subscriber has accepted a certificate after the subscriber has the following actions:

1) the subscriber has downloaded and installed the certificate; or

2) with the permission of the subscriber, iTrusChina RA has downloaded the certificate on behalf of the subscriber and sent the certificate to the subscriber by email; or

3) after iTrusChina sends the certificate acquisition notice to the subscriber, the subscriber does not refuse within the agreed time.

4.4.2 Publication of the Certificate by the CA

Publication of the certificate starts from iTrusChina sending the certificate to the subscriber. iTrusChina will publish the certificate to Certificate Transparency Log as per requirements from Google and Apple.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

iTrusChina and its RA do not notify other entities of issued certificates.

4.5 Key Pair and Certificate Usage

Key pairs and certificates shall not be used for purposes other than those specified and approved uses, otherwise their application will not be protected by relevant laws and iTrusChina's CP.

4.5.1 Subscriber Private Key and Certificate Usage

The actions of submitting a certificate application and accepting the certificate issued by iTrusChina shall be deemed the subscriber has agreed to abide by the terms and conditions of rights and obligations related to iTrusChina and the relying parties. After a subscriber receives a digital certificate, the subscriber shall take reasonable measures to properly keep the corresponding private key of the certificate to avoid unauthorized use.

Subscribers shall protect their private keys from unauthorized use and shall not use expired or revoked certificates. Private keys should not be archived.

Regarding a SSL certificate, the subscriber has the responsibility and obligation to ensure that the certificate is only deployed in the server that the Subject Alternative Name listed in the certificate corresponds to.

4.5.2 Relying Party Public Key and Certificate Usage

After a relying party receives information loaded with a digital signature, it is obligated to perform the following verification operations:

1) obtaining the certificate and trust chain corresponding to the digital signature;

2) confirming that the certificate corresponding to the signature is a certificate trusted by the relying party;

3) confirming whether the certificate corresponding to this signature has been revoked by querying CRL or OCSP;

4) confirming the purpose of the certificate is applicable to the corresponding signature;

5) verifying the signature with the public key in the certificate.

If the above conditions are not satisfied, the relying party is liable to reject the signature information.

4.6 Certificate Renewal

Certificate renewal refers to issuing a new certificate to a subscriber without changing the subject information of the certificate before the subscriber's certificate expires.

4.6.1 Circumstance for Certificate Renewal

The subscriber's certificates issued by iTrusChina can be renewed 30 days ahead of the certificate expiry date. Within this period, subscribers can apply for certificate renewal at iTrusChina's certificate service sites or the RA. For SSL certificates, the subscribers can apply for certificate renewal without updating keys.

4.6.2 Who may Request Certificate Renewal

The same as Section 4.1.1 of this CP.

4.6.3 Processing Certificate Renewal Requests

The same as Section 4.2 of this CP.

4.6.4 Notification of New Certificate Issuance to Subscriber

The same as Section 4.3.2 of this CP.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The same as Section 4.4.1 of this CP.

4.6.6 Publication of the Renewal Certificate by the CA

The same as Section 4.4.2 of this CP.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The same as Section 4.4.3 of this CP.

4.7 Certificate Re-Key

Certificate re-key refers to generate a new key pair, use the same subject distinguished name as the original certificate and issue a new certificate by the same issuer.

4.7.1 Circumstance for Certificate Re-key

The same as Section 3.3 of this CP.

4.7.2 Who may Request Certification of a new Public Key

The same as Section 4.1.1 of this CP.

4.7.3 Processing Certificate Re-Keying Requests

iTrusChina handles certificate re-keying requests through the certificate renewal request handling process as described in Section 4.6.3 of this CP.

4.7.4 Notification of New Certificate Issuance to Subscriber

The same as Section 4.3.2 of this CP.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The same as Section 4.4.1 of this CP.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The same as Section 4.4.2 of this CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The same as Section 4.4.3 of this CP.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Certificate modification refers to the application for a new certificate due to change of information other than the subject information and the valid period of the existing certificate. When the certificate is modified, iTrusChina will re-verify certificate information and only the modified information will be authenticated if the certificate application materials are within the valid period (398 days for OV and EV certificate application material) and can be directly used. If the above certificate application materials have expired, iTrusChina will

re-authenticate and re-verify all the information. Only after they pass the authentication and verification will iTrusChina reissue a new certificate.

4.8.2 Who may Request Certificate Modification

Only certificate subscribers or authorized representatives of certificate subscribers within a valid period can request certificate modifications. iTrusChina does not provide certificate modification services to all subscribers.

4.8.3 Processing Certificate Modification Requests

The same as Section 4.2 of this CP.

4.8.4 Notification of New Certificate Issuance to Subscriber

The same as Section 4.3.2 of this CP.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The same as Section 4.4.1 of this CP.

4.8.6 Publication of the Modified Certificate by the CA

The same as Section 4.4.2 of this CP.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The same as Section 4.4.3 of this CP.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Certificate Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

iTrusChina shall revoke a certificate in 24 hours if one or more of the following occurs:

1) the subscriber requests revocation of the certificate in writing;

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

3) iTrusChina obtains evidence that the subscriber's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements in sections 6.1.5 and 6.1.6 of Baseline Requirements;

4) iTrusChina obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

5)iTrusChina obtains evidence that the certificate was misused;

6) iTrusChina is made aware that the subscriber has violated one or more of its material obligations under the subscriber agreement and CP/CPS;

7) iTrusChina is made aware of any circumstance indicating that use of a FQDN or IP address is no longer legally permitted (for example, a court or an arbitrator has revoked the domain name registrant's right to use the domain name, relevant licenses and service agreements of the domain name registrant and the applicant have terminated, or the domain name registrant fails to renew the domain name).

8) iTrusChina is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subdomain name;

9) iTrusChina is made aware of a material change in the information contained in the certificate;

10) iTrusChina is made aware that the certificate was not issued in accordance with Baseline Requirements, or this CP, or the corresponding CPS;

11) iTrusChina believes any information in the certificate is inaccurate, untrue or misleading;

12) iTrusChina ceases operations for any reason and has not made agreements for another CA to provide revocation support for the certificate;

13) iTrusChina's right to issue certificates as per Baseline Requirements expires or is revoked or terminated, unless it continues to maintain the CRL/OCSP Repository;

14) Revocation is required by iTrusChina's Certificate Policy and/or Certification Practice Statement;

15) iTrusChina is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed.;

16) The fulfilment of obligations in CPS is delayed or impeded by force majeure; natural disasters; computer or communication failure; changes in laws and regulations;

government actions; or other causes that are beyond individual control and pose a threat to information of others;

17) After iTrusChina has fulfilled its obligation to remind payment, the subscriber still fails to pay the fee for services.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

iTrusChina shall revoke a subordinate CA certificate within 7 days if one or more of the following occurs:

1) the subordinate CA formally requests revocation of the certificate in writing;

2) the subordinate CA has found and notifies the root CA that the original certificate request is not authorized and does not retroactively grant authorization;

3) iTrusChina obtains evidence that the subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements in sections 6.1.5 and 6.1.6 of Baseline Requirements;

4) iTrusChina obtains evidence that the certificate was misused;

5) iTrusChina is made aware that the subordinate certificate was not issued in accordance with Baseline Requirements, or the subordinate CA fails to comply with the CP/CPS;

6) iTrusChina believes any information in the certificate is inaccurate, untrue or misleading;

7) iTrusChina ceases operations for any reason and has not made agreements for another CA to provide revocation support for the certificate;

8) iTrusChina's right to issue certificates as per Baseline Requirements expires or is revoked or terminated, unless it continues to maintain the CRL/OCSP repository;

9) this CP or the corresponding CPS requires to revoke the subordinate CA certificate;

4.9.2 Who can Request Revocation

The subscriber, iTrusChina and its RA, or judicial personnel authorized by judicial authorities can initiate revocation. In addition, relying parties, application software providers, anti-virus agencies or other third parties may submit certificate problem reports to inform iTrusChina of reasonable cause to revoke the certificate.

4.9.3 Procedures for Revocation Request

4.9.3.1 A Subscriber Makes an Application for Revocation on One's Own Initiative

1) the subscriber submits the application form for revocation and identification paper to iTrusChina and explains reasons for revocation;

2) iTrusChina verifies the certificate revocation request based on the provisions in Section 3.4 of this CP, and carries out the revocation if the request passes the verification.

3) iTrusChina publishes the result to the certificate revocation list in time after the revocation;

4) iTrusChina notifies the subscriber of revocation of the certificate and reasons for the revocation via telephone, email or other proper means; in the case of failing to contact with the subscriber, iTrusChina will announce the revoked certificate through websites if necessary;

5) iTrusChina provides 7*24 hours certificate revocation application service. the application method will be explained in the CPS.

4.9.3.2 A Subscriber Is Forced to Revoke a Certificate

1) when iTrusChina has sufficient reason to believe any circumstance described in Section 4.9.1.1 of this CP that will lead to compulsory revocation of a subscriber certificate, the revocation can be carried out after approval from iTrusChina Security Policy Administration Committee;

2) when security risks arise from the private keys corresponding to the Root certificate or the subordinate CA certificate of iTrusChina, the subscriber certificate revocation can be carried out directly after approval of national digital certification service authorities;

3) when third parties such as relying parties, judicial organizations, application software providers, anti-virus agencies, etc. submit certificate problem reports, iTrusChina shall organize an investigation and determine whether to revoke the certificate according to the investigation result, if iTrusChina confirms that the certificate needs to be revoked through investigation, the period from receipt of the certificate problem report to the revocation of the certificate shall not exceed the period specified in 4.9.1.

4) iTrusChina or RA will notify the subscriber of revocation of the certificate and reasons for the revocation via telephone, email or other proper means. In case of failing to contact with the subscriber, iTrusChina will announce the revoked certificate through websites if necessary.

4.9.4 Revocation Request Grace Period

iTrusChina does not allow grace periods of revocation requests.

4.9.5 Time Within which CA must Process the Revocation Request

Within 24 hours upon the receipt of a certificate problem report, iTrusChina or RA shall investigate contents of the certificate problem report to decide whether to revoke the certificate or take other proper actions.

If iTrusChina confirms that the certificate needs to be revoked through investigation, the period from receipt of the certificate problem report to the revocation of the certificate shall not exceed the period specified in 4.9.1.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties shall check whether their trusted certificates are revoked through the OCSP service or CRL query provided by iTrusChina.

4.9.7 CRL Issuance Frequency

For the subscriber certificates, the CRL publication cycle of iTrusChina shall not exceed 96 hours, i.e., releasing the latest CRL within 4 days. Subscriber CRLs are valid for up to 10 days.

For the subordinate CA certificates, the CRL publication cycle of iTrusChina shall not exceed 12 months. If a subordinate CA certificate is revoked, iTrusChina will update the CRL within 24 hours after the revocation. The CRL of subordinate root is valid for a maximum of 12 months.

4.9.8 Maximum Latency for CRLs

The maximum latency for CRL publication of iTrusChina is within 24 hours after the publication cycle.

4.9.9 On-line Revocation/ Status Checking Availability

iTrusChina shall provide certificate subscribers and relying parties with online certificate status protocol (OCSP) services. OCSP service of iTrusChina meets the requirements of RFC6960 and are signed with special OCSP service certificates.

4.9.10 On-line Revocation Checking Requirements

Users can freely query online status with no limit on read access set by iTrusChina.

iTrusChina provides two ways for OCSP query service: Get and Post.

For the status of subscriber certificates, iTrusChina updates OCSP information at least every 4 days. OCSP responses have a maximum expiration time of 7 days.

For the status of subordinate CA certificates, iTrusChina updates OCSP information at least every 12 months and within 24 hours after revoking a subordinate CA certificate.

When receiving a request for status of a certificate that has not been issued, iTrusChina does not respond with a "good" status.

4.9.11 Other Forms of Revocation Advertisements Available

Apart from CRL or OCSP servers for certificate revocation information query, iTrusChina does not provide other publication forms of revocation information.

4.9.12 Special Requirements Related to Key Compromise

Any subscriber or RA who has found the security of a certificate’s key is compromised shall immediately request revocation of the certificate from iTrusChina. If the security of a CA key (root CA or subordinate CA key) is compromised or is suspected to be compromised, iTrusChina will inform the subscriber and relying parties timely in a proper manner within a reasonable time.

4.9.13 Circumstances for Certificate Suspension

iTrusChina does not support certificate suspension.

4.9.14 Who can Request Certificate Suspension

Not applicable.

4.9.15 Procedures for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

iTrusChina provides certificate status query services through CRL and OCSP and warranties reasonable response time and concurrent processing capability for query requests.

4.10.1 Operational Characteristics

Regarding a revoked certificate, iTrusChina does not delete its revocation records from OCSP server; iTrusChina does not delete its revocation records from CRL until the certificate expires. iTrusChina's certificate status query is provided in the form of network service:

- For CRL, it is provided using HTTP protocol;
- For OCSP, it is provided in compliance with RFC6960.

4.10.2 Service Availability

Both CRL and OCSP certificate status query services of iTrusChina are 7 * 24 available and designed to minimize downtime. The response time is no more than 10 seconds (no more than 3 seconds for the CRL response time for EV certificates; The response time here does not include the time-consuming of obtaining data slowly due to reasons such as the subscriber network.), which means: with good network, subscribers and relying parties can get real-time responses for the certificate status query service.

4.10.3 Optional Features

None.

4.11 End of Subscription

End of subscription includes the following circumstances:

1) a certificate is not renewed after expiration;

2) a certificate is revoked before expiration.

Once a user terminates the use of certification service of iTrusChina within the valid period of the certificate, iTrusChina will revoke the certificate of the subscriber after approving the subscriber's termination request, and publish it in accordance with CRL publication policy; iTrusChina records the operation process of certificate revocation in details and regularly archives the certificates of those subscribers who end subscription and the relevant subscriber data.

4.12 Key Escrow and Recovery

iTrusChina does not hold any private key in escrow for SSL certificate subscribers, thereby not providing key recovery service.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Policy and Practices of Session Key Encapsulation and Recovery

Not applicable.

5. Facility, Management, Operational and Physical Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The operating site of iTrusChina is mainly divided into four areas according to their functions, which are public area, service area, management area and core area. In the core area, there is a high-performance electromagnetic shielding enclosure where CA servers, database systems and key management objects like cryptographic devices, etc. are placed.

5.1.2 Physical Access

Any entry and exit action to every physical security layer of iTrusChina needs to be recorded, audited and controlled, thereby ensuring that everyone that accesses to each physical security layer has been authorized. iTrusChina's CPS shall make detailed regulations on physical access control.

5.1.3 Power and Air Conditioning

iTrusChina shall have a safe and reliable power supply system and a power reserve system to ensure that systems could provide normal services for 7*24 hours. Besides, iTrusChina has heating/ventilating/air-conditioning systems to control the temperature and humidity of operating facilities.

5.1.4 Water Exposures

Machine rooms of iTrusChina shall take reasonable precautions to minimize the impact of water exposure to the CA system.

5.1.5 Fire Prevention and Protection

Machine rooms of iTrusChina shall adopt preventive measures and formulate relevant programs to eliminate and prevent fire, and these fire prevention measures shall conform to security requirements of the local fire management department.

5.1.6 Media Storage

The storage and use of physical medium shall satisfy security requirements on fireproofing, waterproofing, etc., and strict protective measures shall be taken to prevent unauthorized use and access to medium.

5.1.7 Waste Disposal

iTrusChina shall shred sensitive files and materials out of use before processing to make the information unrecoverable. Before the disposal, cryptographic devices shall be initialized first and then be destroyed physically as per the method provided by the manufacturer.

5.1.8 Off-site Backup

iTrusChina makes off-site backups for critical system data and audit log data, and the security level of backup locations shall be no lower than the production environment.

5.2 Procedural Controls

5.2.1 Trusted Roles

In the process of providing certification service, roles that essentially affect key operations, such as certificate issuance, use, administration, revocation, etc. will be regarded as trusted roles by iTrusChina. These roles include but are not limited to:

1) Key and cryptographic devices personnel, which are responsible for the management of CA keys, certificates life-cycle and cryptographic devices;

2) Validation and customer service personnel, which are responsible for the validation of subscriber certificates, and customer support services;

3) System maintenance personnel, which are responsible for the maintenance of the hardware and software of CA system;

4) Security management personnel, which are responsible for the area security and daily physical security management;

5) Security audit personnel, which are responsible for the audit of the operations;

6) Human resource management personnel, which are responsible for conducting the background investigation on trusted roles and the management of personnel security.

5.2.2 Number of Individuals Required per Task

iTrusChina has strict control procedures for service operation process. In accordance with the policy of separation of duties specified in Section 5.2.4 in this CP, iTrusChina shall ensure that an individual couldn't play multiple roles, and that sensitive operations be jointly completed by multiple trusted individuals, which include:

1) The access to the electromagnetic shielding area should be a dual access;
2) The safe box for saving the activation data of the root key is set to dual access；
3) The admin privileges of the cryptographic devices shall use m of n PINs, and each share of the PINs shall be held by different trusted personnel;
4) The super admin password should be split into two segments held by different trusted personnel;
5) The validation shall be processed by at least two trusted personnel.

5.2.3 Identification and Authentication for Each Role

iTrusChina authenticates the physical access of trusted roles by access control cards and fingerprint identification to confirm the corresponding permission.

Trusted roles of iTrusChina and RA who perform the subscriber certificate life cycle management work shall use the corresponding digital certificate for their access to the system and complete the certificate management work.

System maintenance personnel shall use their own accounts and passwords to log in the system in a bastion host for maintenance.

5.2.4 Roles Requiring Separation of Duties

Separation of duties means that if one person plays a role of one function, he or she shall not play the role of another special function. iTrusChina implements the policy of separation of duties on the following roles:

(NO means not to be concurrent)

	Key and cryptographic devices personnel	Validation and customer service personnel	System maintenance personnel	Security management personnel	Security audit personnel	Human resource management personnel
Key and cryptographic devices personnel	——	NO	NO	NO	NO	NO
Validation and customer service personnel	NO	——	NO	NO	NO	NO
System maintenance personnel	NO	NO	——	NO	NO	NO
Security management personnel	NO	NO	NO	——	NO	NO
Security audit personnel	NO	NO	NO	NO	——	NO
Human resource management personnel	NO	NO	NO	NO	NO	——

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

iTrusChina has the following qualification requirements for the personnel who play trusted roles:

1) Have good social and work backgrounds;

2) Abide by national laws and regulations with no criminal record;

3) Abide by iTrusChina's regulations, norms and systems related to security management;

4) Have responsible and conscientious working attitude and favourable working experience;

5) Have good team work spirit.

5.3.2 Background Check Procedures

In order to ensure the personnel with trusted roles to be qualified for the relevant work, iTrusChina will firstly conduct background investigation on employees in accordance with *iTrusChina's Policy of Trusted Employees*. Background investigation conforms to the requirements of laws and regulations, verifies the background information through relevant organizations and departments as far as possible and protects individual privacy.

All trusted employees and trusted employees who apply for transfer-in shall provide written consent to the background investigation. Background investigation is divided into: basic investigation and advanced investigation.

Basic investigation includes investigations on work experience and educational background.

Advanced investigation also includes investigations on criminal records, apart from items of basic investigation.

Investigation procedures include:

1) HR department is responsible for confirming the personal materials of the applicants. The following materials shall be provided: CV, graduation certificate of highest education, qualification certificates, ID, etc.

2) HR department identifies the authenticity of the provided materials by telephone and network, etc.

3) In the background investigation, the qualification to become a trusted person can be directly rejected for those who perform any one of the following behaviours:

- The act of fabricating facts or materials;
- With the aid of the proof of unreliable personnel;
- The use of illegal identity certificates, education, or qualification certificates;
- There is a serious dishonesty at work.

4) After completing the investigation, HR department will report the results to the leaders in charge of related work for approval.

5) iTrusChina signs a confidentiality agreement with its employees to restrain employees from divulging all confidential and sensitive information of CA certificate service.

5.3.3 Training Requirements

In order to make the relevant personnel competent for their work, iTrusChina has a special training program for all the personnel of the trusted roles. The training contents include:

1) CP and CPS issued by iTrusChina;

2) Basic knowledge of PKI;

3) iTrusChina's operation management system, technical system and security rules;

4) Description of job duties and posts.

5.3.4 Retraining Frequency and Requirements

iTrusChina shall arrange retraining as needed so as to ensure that the employees of important positions be more qualified for their job requirements to successfully fulfil their duties.

5.3.5 Job Rotation Frequency and Sequence

The job rotation frequency and sequence of iTrusChina's in-service personnel shall be decided according to the internal work arrangement.

5.3.6 Sanctions for Unauthorized Actions

iTrusChina has established and maintained a set of management measures to punish unauthorized actions, including rescinding or terminating labour contracts, removing from

posts of duty, fines, and criticizing and educating, etc. These sanctions should comply with the requirements of laws and regulations.

5.3.7 Independent Contractor Requirements

For people who do not belong to iTrusChina's internal personnel yet they are engaged in the work related to certificate validation, iTrusChina requires the same skill level as the internal personnel of the corresponding position.

5.3.8 Documentation Supplied to Personnel

Documentation supplied to personnel generally include CP, CPS, employee guidelines, job description, work process and procedure specification, etc.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

iTrusChina shall record the following types of events:

- CA certificate and key lifecycle events, including:
  -Key generation, backup, storage, recovery, archival, and destruction;
  -Certificate requests, renewal, and re-key requests, and revocation;
  -Approval and rejection of certificate requests;
  -Cryptographic device lifecycle management events;
  -Generation of Certificate Revocation Lists and OCSP entries;
  -Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
- Subscriber Certificate lifecycle management events, including:

-Certificate requests, renewal, and re-key requests, and revocation;
-All verification activities stipulated in these Requirements and the CA's CPS;
-Approval and rejection of certificate requests;
-Issuance of Certificates; and
-Generation of Certificate Revocation Lists and OCSP entries.

- System operation events, including,

-system start-up and shutdown.

-the creation, deletion, modification of system jurisdiction, and password modification.

These records consist of system logs of the CA system and manual records of operators.

- System security events, including,

-successful or unsuccessful CA system access attempts.

-unauthorized access and access attempt for the CA system network.

-system crashes, hardware failures and other anomalies.

-Installation, update and removal of software on a Certificate System.

-security events recorded by firewalls and routers.

These records consist of auto logs of the system and manual records of operators.

- Work records of iTrusChina sites, for example,

-entry and exit of authorized personnel.

-entry and exit of unauthorized personnel and accompanying persons.

-maintenance operation of site facilities.

These records consist of auto logs of the system and manual records of operators.

Log entries must include the following elements:

- Date and time of entry.
- The registered serial number or ordinal number for auto entry record.
- Identity of the person making the journal entry.
- Description of the entry.

5.4.2 Frequency of Processing Log

iTrusChina shall check the audit log regularly to find important security and operation events and take corresponding measures for the detected security events.

5.4.3 Retention Period for Audit Logs

iTrusChina keeps the audit log of the CA service properly, and the audit log related to the certificate is retained for at least 2 years after the certificate expired.

5.4.4 Protection of Audit Log

For all audit logs, strict physical and logical access control measures shall be taken to prevent unauthorized browsing, alteration, deletion, etc.

5.4.5 Audit Log Backup Procedures

The audit log shall be backed up periodical.

5.4.6 Audit Collection System

Regarding the electronic audit information, iTrusChina's log server can collect and archive the following logs:

1) certificate management system;

2) certificate issuing system;

3) certificate accepting system;

4) access control system;

5) database system;

6) other systems that need to be audited.

Regarding paper audit information, there is a special filing cabinet for collection and archival.

5.4.7 Notification to Event-Causing Subject

When iTrusChina detects the attack, it will record the attacker's behaviours, trace the attacker to the extent permitted by the law, and retain the right to take the corresponding countermeasures. iTrusChina has the right to decide whether to notify subjects related to the event.

5.4.8 Vulnerability Assessment

According to the requirements of CA/B Forum NCSSR, iTrusChina scans the system for vulnerabilities every 3 months and conducts a penetration test every year.

According to audit records, iTrusChina regularly carries out security vulnerability assessment and takes remedial measures based on the assessment report.

5.5 Records Archival

5.5.1 Types of Records Archived

iTrusChina archives the following types of records:

1) Documents of certificate system building and upgrading;

2) Certificates

3) Life cycle management records of subscriber certificates;

4) Audit records;

5) CP and CPS;

6) Employee materials, including but not limited to materials of background investigation, employment, training, etc.;

7) Various external and internal evaluation documents.

5.5.2 Retention Period for Archive

iTrusChina' CPS shall stipulate a reasonable period for retaining archived records.

5.5.3 Protection of Archive

The archived data shall be protected by proper physical and logical access control methods, and only authorized trusted personnel are allow for the access to the archived data to prevent unauthorized browsing, alteration, deletion, or other tampering behaviours.

5.5.4 Archive Backup Procedures

Backups of electronic archiving records generated by the system shall be made regularly and backup files shall be stored in different places; the manual electronic records shall be archived in SVN. Backups of written archived materials are not required, but strict measures shall be taken to ensure their security.

5.5.5 Requirements for Time-stamping of Records

iTrusChina doesn't adopt the time-stamping technology for logs.

5.5.6 Archive Collection System

iTrusChina and RA shall build an internal archive collection system.

5.5.7 Procedures to Obtain and Verify Archive Information

iTrusChina shall take proper access control methods to ensure that only the authorized personnel can approach the archive information and strictly prohibit unauthorized operations such as access, reading, alteration and deletion, etc.

5.6 Key Changeover

When the lifetime of the key pair that corresponds to the CA certificate exceeds the maximum life cycle specified in this CP, iTrusChina will start the key renewal process and replace the already expired CA key pair. Even within the life cycle of a key pair, iTrusChina can also generate a new CA certificate through the generation of a new key pair. Before a CA certificate expires, the key changeover process will be activated to ensure the smooth transition of the entity in the CA system from the old key pair of the CA to a new key pair.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

iTrusChina shall formulate various accident handling plans and emergency response plans and stipulate the corresponding incident and compromise handling procedures.

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

If computer resources, software, and/or data are corrupted, iTrusChina shall immediately start the accident handling procedures, and if necessary, the recovery can be implemented in accordance with the disaster recovery plan.

5.7.3 Recovery Procedures After Key Compromise

iTrusChina will handle the compromise of entity certificate private key in line with the following procedures:

1) When the certificate subscriber finds that the entity certificate private key is compromised, the subscriber must immediately stop using the private key and immediately visit certificate service sites of iTrusChina or its RA to revoke the certificate, or immediately notify iTrusChina or its RA to revoke the certificate by telephone, etc., and reapply for a new certificate according to the relevant process. iTrusChina will issue certificate revocation information according to Section 4.9 of this CP.

2) When iTrusChina or RA finds that the entity certificate private key of the subscriber certificate is compromised, iTrusChina or RA will immediately revoke the certificate and notify the certificate subscriber; the subscriber must immediately stop using the private key

and reapply for a new certificate according to the relevant process. iTrusChina will issue certificate revocation information according to Section 4.9 of this CP.

3) When the private key of iTrusChina's root CA or subordinate CA is compromised, iTrusChina will handle the emergency according to key emergency plan, and notify the relying party and application software supplier including Mozilla/Microsoft/Apple/Google/360 through email immediately.

5.7.4 Business Continuity Capabilities after a Disaster

In the event of a disaster, iTrusChina shall have the following capabilities to continue the business:

1. Resume the service system in the shortest possible time, no more than 72 hours;

2. Being able to restore customer information;

3. Being able to ensure that the operation site after recovery conform to safety requirements;

4. Have sufficient personnel to continue services and do not violate the requirements of separation of duties.

5.8 CA or RA Termination

When iTrusChina and its RAs need to stop their business, they will work strictly in accordance with the requirements of *Electronic Signature Law of the People's Republic of China* and the relevant regulations on the business suspension for certification authorities.

Before the termination, iTrusChina shall:

1) Determine the service undertaking unit;

2) Draft the termination statement;

3) Notify the relevant entities;

4) Process the archive records;

5) Stop the service of CA system;

6) Archive relevant system logs;

7) Process and store sensitive documents.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

iTrusChina's keys are generated using the cryptographic devices approved and licensed by the State Cryptography Administration, and key generation, management, storage, backup and recovery done by the devices follows relevant regulations of FIPS140-2 Standard. Since China has strict administration requirements on cryptographic products, FIPS140-2 Standard is not a standard approved and supported by the State Cryptography Administration, FIPS140-2 Standard is only enforced as reference, selectively applicable on the premise of passing the evaluation and certification of the State Cryptography Administration and being licensed by national cryptography administration policies. For specific reference, please refer to materials provided by the device manufacturer.

The process of CA key pair generation is witnessed by special key managers and several reliable employees of iTrusChina and auditors of an independent third party, and is completed in shielding computer rooms of iTrusChina in accordance with iTrusChina Key Ceremony. iTrusChina Key Ceremony stipulates the process control of CA key generation and participants.

6.1.1.2 Subscriber Key Pair Generation

Subscriber's key pairs are generated by the built-in key generation mechanism of subscriber's server or other devices.

iTrusChina does not generate key pairs for Subscribers.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber shall electronically submit the public key to iTrusChina for certificate issuing, using the file package of certificate signing request information in PKCS#10 format or other

digital signature on Subscriber's own or through registration authority. When network transmission is needed, Secure Sockets Layer (SSL) and other secure protocols shall be used.

6.1.4 CA Public Key Delivery to Relying Parties

iTrusChina shall deliver CA public key to relying parties in a secure and reliable way, for example, downloading from secure sites, etc.

6.1.5 Algorithm type and Key Sizes

Certificates MUST meet the following requirements for algorithm type and key size：

Root CA Certificates：

digest algorithm：SHA256 or SHA384

RSA modulus size：not less than 2048,

ECC modulus size：not less than 256.

Subordinate CA Certificates：

digest algorithm：SHA256 or SHA384

RSA modulus size：not less than 2048,

ECC modulus size：not less than 256.

Subscriber Certificates：

digest algorithm：SHA256 or SHA384

RSA modulus size：not less than 2048,

ECC modulus size：not less than 256.

iTrusChina will adjust the algorithm type and the key size according to the BR and standards issued by State Cryptography Administration of China.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall be generated by using the cryptographic hardware and media with the license from the State Cryptography Administration and shall follow generation norms and standards of these devices.

Regarding the parameter quality check, since keys are generated and stored using the cryptographic hardware and media with the license from State Cryptography Administration, the parameters have already met the requirements on high security level.

6.1.7 Key Usage Purposes

X.509v3 certificate issued by iTrusChina includes key usage extensions, and their usage conforms to RFC5280 Standard. Regarding the purposes specified by iTrusChina in key usage extensions of the issued certificate, the certificate Subscriber shall use the key according to specified purposes.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

iTrusChina shall ensure the security of CA private keys through the comprehensive realisation of physical, logical and process control. Subscriber agreement will require certificate subscribers to adopt necessary prevention measures so as to avoid the loss, disclosure, alteration or unauthorized use of private key.

6.2.1 Cryptographic Module Standards and Controls

iTrusChina keys shall be generated using the cryptographic device approved and licensed by the State Cryptography Administration, and key generation, management, storage, backup and recovery done by the devices follows relevant regulations of FIPS140-2 Standard. Since China has strict management requirements on cryptographic products, yet FIPS140-2 Standard is not a standard approved and supported by the State Cryptography Administration, FIPS140-2 Standard is only enforced as reference, selectively applicable on the premise of passing the evaluation and certification of the State Cryptography Administration and being licensed by national cryptography management policies. For specific reference, please refer to materials provided by the device manufacturer.

6.2.2 Private Key (n out of m) Multiple-person Control

iTrusChina shall realize the operation of CA cryptographic devices jointly participated by multiple reliable personnel through technical and procedural control mechanism. For technical mechanism, the technology of 'secret splitting' can be used, i.e. splitting the management jurisdiction data required for CA private key into several parts, which are in separate possession of multiple reliable personnel. If the secret splitting sum of one hardware cryptographic module is m, only when the number of reliable personnel exceeds n can the CA private key stored on the cryptographic module be backed up.

6.2.3 Private Key Escrow

iTrusChina neither allows escrow for the root private key or CA private key, nor provides escrow service of private key for subscribers.

6.2.4 Private Key Backup

In order to ensure continued service development, iTrusChina has to create backups of CA private keys in case of disaster recovery use. iTrusChina has two kinds of backups for the root private key and the CA private key. One is to generate the backup ciphertext files and backup authority recovery IC cards according to the operation specification provided by the cryptographic device manufacturer and save them in the safe box in the shielding machine room(or bank safe deposit box and other location that security levels are not lower than the local backup); one is to generate a cloning device according to the operation specification provided by the cryptographic device manufacturer(or bank safe deposit box and other location that security levels are not lower than the local backup). Cryptographic module (i.e. cryptographic device) that stores CA private keys shall conform to the requirements specified in Section 6.2.1 of this CP. Copying CA private keys to the backup hardware cryptographic module shall meet the requirements specified in Section 6.2.6 of this CP.

Regarding subscriber certificates, if the cryptographic module that stores the certificate private keys allows private key backup, iTrusChina suggests subscribers to make backups of private keys and protect the backup private keys by adopting passwords or other access control mechanisms so as to prevent from unauthorized alteration or disclosure.

6.2.5 Private Key Archival

When CA key pairs of iTrusChina go beyond the service life, these CA key pairs shall be archived and retained for at least 7 years. The archived CA key pairs are retained on the hardware cryptographic module mentioned in Section 6.2.1 of this CP.

iTrusChina or registration authority does not archive private keys of subscriber certificates; if subscriber's cryptographic module that retains certificate private keys allows backup of private keys, iTrusChina suggests subscribers to archive private keys and protect the archived private keys by adopting passwords or other access control mechanisms so as to prevent from unauthorized disclosure.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys of iTrusChina shall make backups in strict accordance with root key management practices, apart from which, any import or export operation is not allowed. When a CA key pair has been backed up to other hardware cryptographic module, it is transmitted between modules in an encrypted form, and identity authentication is required before transmission so as to avoid the loss, theft, alteration, unauthorized disclosure and unauthorized use of CA private keys.

Regarding subscriber certificates, if the used cryptographic module (software or hardware) supports the transfer of private keys, iTrusChina requires that Subscriber shall use secure passwords to protect private keys for transfer; moreover, Subscriber shall ensure that the exported private keys are protected against any loss, theft, alteration, unauthorized disclosure, unauthorized use, etc.

6.2.7 Private Key Storage on Cryptographic Module

iTrusChina private keys shall be stored on the hardware cryptographic module that meets the requirements of the State Cryptography Administration in an encrypted form, and the use of private keys shall also be conducted on the hardware cryptographic module.

Regarding subscriber certificates, Subscriber shall store private keys on the cryptographic module approved by the State Cryptography Administration (including SSL accelerator cards), and the cryptographic module that stores private keys shall be under control of Subscriber. Subscriber needs to adopt the corresponding security measures to prevent from unauthorized access, acquisition or use of private keys, and such measures include that the use of private keys shall be protected by passwords, server and cryptographic module shall be located in secure and controllable physical environment, etc.

6.2.8 Method of Activating Private Keys

iTrusChina private keys shall be stored on the hardware cryptographic module, and the activation shall be conducted by operation authority according to Section 6.2.2 of this CP. When the CA private key (in the online or offline cryptographic module) is needed for using, the key manager needs to provide the operation IC card to accomplish the activation.

Private keys of subscriber certificate that are saved on the cryptographic module can be activated and used only after the user inputs key protection information (activation data), such as password (or PIN code) or fingerprint, etc.

6.2.9 Method of Deactivating Private Keys

Regarding private keys of iTrusChina, when CA system sends logout instruction to the cryptographic module or when the cryptography management software sends close instruction to the cryptographic module, or when the hardware cryptographic module that stores private keys is power off, private keys enter the inactivated state.

Subscriber deactivates the activated state of private key at the Subscriber's sole discretion, and when the service program is closed, or when the system is logged off, or when the system is power off, private keys then enter the inactivated state.

6.2.10 Method of Destroying Private Keys

When private keys are out of use or have no need to be saved, private keys shall be destroyed so as to avoid loss, theft, disclosure or unauthorized use.

Regarding private keys of subscriber certificate that are out of use, private keys shall be destroyed so as to avoid loss, theft, disclosure or unauthorized use. In case of using private keys for information decryption after the expiry of these private keys or the revocation of the corresponding certificates, the end user shall properly keep private keys for a certain period of time for the convenience of decrypting the encrypted information. If there is no need to save private keys, private keys will be destroyed through deleting private keys or initializing the system or the cryptographic module.

6.2.11 Cryptographic Module Rating

iTrusChina shall use cryptographic products approved and licensed by State Cryptography Administration, and State Cryptography Administration is responsible for the evaluation of cryptographic modules.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

iTrusChina shall archive certificates by storing them in the database and making offsite backup. The integrity of the backup data is verified periodically.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period of the CA certificate is no more than 25 years, and the subscriber SSL certificate is valid for a maximum of 398 days.

Usage period of public key and private key is related to yet different from the certificate validity period.

Regarding certificates used for signing, their private keys can only be used for digital signature within the certificate validity period, and the usage period of private keys shall not go beyond the certificate validity period. However, in order to ensure that information signed within the certificate validity period can be verified, the usage period of public keys can go beyond the certificate validity period.

Regarding certificates used for encryption, their public keys can only be used for information encryption within the certificate validity period, and the usage period of public keys shall not go beyond the certificate validity period. However, in order to ensure that information encrypted within the certificate validity period can be decrypted, the usage period of private keys can go beyond the certificate validity period.

Regarding certificates used for identity authentication, their private keys and public keys can only be used within the certificate validity period.

When a certificate has multiple purposes, the usage period of its public key and private key is the combination of the above cases.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data of CA private key must be strictly generated, distributed and used in accordance with the requirements of regulations about key activation data partitioning and key management.

Regarding the activation data of subscriber's private key, it is suggested that the subscriber should control the activation of the private key by using the dual factor mechanism (such as hardware + password, biometric device + password, etc.).

6.4.2 Activation Data Protection

The activation data of CA private key must be secretly partitioned and managed by different trusted personnel, and the personnel in charge must comply with the requirements of separation of duties.

The activation data of subscribers must be generated in a safe and reliable environment and be kept properly, or be destroyed after being memorized, which must not be known by others. If a certificate subscriber uses a password or PIN code to protect the private key, the subscriber should keep the password or PIN code properly to prevent disclosure or theft. If a certificate subscriber uses biological features to protect the private key, the subscriber should also pay attention to preventing their biological features from theft.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The information security management of CA system formulates comprehensive security management policies and systems to be implemented, reviewed and recorded in operation according to the national standard *Specifications of Cryptography and Related Security Technology for Certificate Authority System, Measures for the Administration of Regulations on Electronic Certification Services* published by the Ministry of Industry and Information Technology, referring to the requirements of the ISO27001 information security management system and other relevant information security standards. The main security technologies and control measures include: identity authentication and verification, logical access control, network access control, etc.

Strict security control measures are adopted to ensure that the system of CA software and data files is secure and trusted with no unauthorized access.

The core system must be physically separated from other systems, and the production system is logically isolated from other systems. This separation can prevent access to the network other than the specified applications. Firewall is used to prevent the invasion of the production system network from the intranet and the extranet, and restrict access to the activities of the production system. Only the trusted personnel in the CA system operation

and management group who need to work and access the system can access the CA database through passwords.

6.5.2 Computer Security Rating

iTrusChina's CA system and its operating environment have been approved by the State Cryptography Administration and Ministry of Industry and Information Technology of the People's Republic of China and obtained the corresponding qualifications.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The CA software of iTrusChina is purchased from qualified commercial CA software provider in China. iTrusChina should control the work of bring the certification system online by changing the internal control process, and require the operation and maintenance personnel to strictly follow the approval and online process execution, in order to assure the security and availability of the system.

iTrusChina will develop validation system for RA API; the software and hardware used in the development of validation system should be deployed in secure controlled environment, and the process of developing and testing should comply with the specification defined and documented by iTrusChina. The going online of this kind of system should also follow the internal change control process mentioned above, and then the operation and maintenance personnel shall execute the process.

6.6.2 Security Management Controls

iTrusChina should formulate various security policies, management regulations and processes for the safety management of the certification system.

The information security management of the certification system should strictly follow the relevant operation and management regulations of the State Cryptography Administration.

The use of the certification system should have strict control measures. All systems have been strictly tested and verified for secure use, and any modification and upgrading will be recorded.

iTrusChina should regularly perform security check on the system to identify whether the device is being invaded, whether there are security vulnerabilities, etc.

6.6.3 Life Cycle Security Controls

iTrusChina should control the certification system's research and development as well as launching through the internal change control process to ensure the security and reliability of the system.

6.7 Network Security Controls

iTrusChina's certification system should adopt firewall to implement access control, IDS/IPS to resist network attack, bastion host to manage the authority of remote-logging, and router to layer the intranet.

All systems of iTrusChina related to certificate issuance adopt multi-factor authentication.

The certification system should only open to specific services and personnel with the minimum access authority.

The certification system should regularly scan security vulnerabilities, check the configuration of security devices, and audit the system logs.

iTrusChina's network security control complies with CA/B Forum NCSSR.

6.8 Time-stamping

The digital certificate and CRL issued by iTrusChina's certification system shall contain time and date information, and these time and date information shall be digitally signed.

All system logs and operation logs should have corresponding time records. These time records do not require the use of digital timestamp technology based on cryptography.

The time source of certification system shall be the national trusted standard time.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

The certificate issued by iTrusChina should comply with ITU-T X.509v3 and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL structure.

iTrusChina generates a non-sequential certificate serial number containing at least 64 bits from a CSPRNG.

7.1.1 Version Number(s)

Certificates must be of type X.509 V3, and the version information is stored in the certificate version format column.

7.1.2 Certificate Extensions

The certificate issued by iTrusChina should comply with the RFC5280 Standard and comply with the requirements from Section 7.1.2.1 to Section 7.1.2.5 in CA/B Forum Baseline Requirements.

7.1.3 Algorithm Object Identifiers

In certificates issued by iTrusChina, the identifiers of cryptographic algorithms are sha256RSA, sha384RSA, sha256ECDSA, and sha384ECDSA.

7.1.4 Name Forms

The form and content of the certificate issued by iTrusChina conform to the requirements of RFC5280.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

When using the Certificate Policy extension, the certificate contains the object identifier of the certificate policy, which corresponds to the corresponding certificate category. See the description in Section 1.2 of this CP.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

iTrusChina issues CRL regularly for subscribers and relying parties to query and use.

7.2.1 Version Number(s)

iTrusChina's CRL is formatted in accordance withX.509 V2.

7.2.2 CRL and CRL Entry Extensions

They are consistent with ITU X.509 and RFC5280 regulations.

- **The version number:** it is used to specify the version information of CRL, and iTrusChina adopts the CRL V2 version corresponding to the X.509 V3 certificate.
- **Signature algorithm:** iTrusChina adopts signature algorithms of sha256RSA and sha256ECDSA.
- **Issuer:** the DN name of the designated issuer is composed of the state, province, city, organization, department and general name, etc.
- **Effective date:** specify a date/time value to indicate the time when the CRL is generated.
- **Next Update:** specify a date/time value to indicate the time when the next CRL will be generated (mandatory use of the domain for this standard).

- **Revocation list:** it specifies the list of certificates that have been revoked. This list contains the serial number of the certificate and the date and time when the certificate is revoked.
- **Authority Key Identifier:** this identifier is used to verify the public key signed on the CRL. It can identify different keys used by the same CA.
- **Next CRL Publish:** specify a date/time value to indicate the time when the next CRL will be published.
- Reason Code: Used for intermediate CA certificate CRL to indicate the reason for revocation.

iTrusChina uses the following reason codes as the reason for revocation of the intermediate CA certificate:

Code 2, CA private key compromise

Code 4, certificate superseded (revocation due to misissue or other non-compliance reasons)

Code 5, cessation of operation (revocation due to the intermediate certificate is no longer used.)

7.3 OCSP Profile

The OCSP response issued by iTrusChina's certification system conforms to the RFC6960 Standard, which defines a standard request and response information format to confirm the status of the certificate.

7.3.1 Version Number(s)

The OCSP V1 version defined by RFC6960.

7.3.2 OCSP Extensions

Compliance with RFC6960.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

iTrusChina should perform the audit and assessment as follows:

1) carry out an operational quality assessment quarterly to ensure the reliability, security and controllability of operation services.

2) carry out an internal audit of authentication quarterly and draw at least 3% of certificate samples.

3) carry out an annual BR Self-Assessment according to CA/Browser Forum Baseline Requirements.

4) carry out an annual self-audit of physical control, key management, operation control, and authentication execution, etc. to determine whether the actual circumstance is consistent with the predetermined standards and requirements and take actions according to the results of the review.

5) carry out an annual operation risk assessment to identify internal and external threats, to assess the possibility and compromise of the threats, and to formulate and implement a disposal plan based on the results of the risk assessment.

6) in addition to internal audit and assessment, iTrusChina also employs independent auditing firms to conduct external audits and assessments in accordance with three standards of WebTrust for CA, WebTrust for CA-Extended Validation SSL and WebTrust for CA- SSL Baseline with Network Security.

8.2 Identity/Qualifications of Assessor

Internal audit and assessment are carried out by iTrusChina's internal audit and assessment team.

External audit will be done by the authority with the following qualifications:

- Must be a licensed and certified assessment authority, honoured a good reputation in the industry;
- Have sufficient knowledge in the computer information security system, communication network security requirements, PKI technology, standards and operation;

- Possess professional skills and tools to check the system operating performance;
- Possess the qualification of WebTrust audit.

8.3 Assessor's Relationship to Assessed Entity

The position of internal auditors and the system administrators, business managers and business operators of this organization must not overlap.

The relationship between external assessors and iTrusChina is independent, and there is no stake between them that may affect the objectivity of the assessment.

8.4 Topics Covered by Assessment

The internal audit shall involve the following schemes:

1) whether the operation process and system are strictly observed.

2) whether the certification service is done strictly according to CP, CPS, service specifications and security requirements.

3) whether all kinds of logs and records are integrated and whether there are any problems;

4) whether there is any other potential security risk.

In accordance with the requirements of WebTrust , the third-party auditors audit iTrusChina independently.

8.5 Actions Taken as A Result of Deficiency

Regarding problems in the internal audit results, the audit assessment team is responsible for overseeing the improvement of the responsible departments.

After the completion of the third-party Auditor's assessment, iTrusChina will rectify and reform in accordance with the work report and accept re-audit and assessment.

8.6 Delivery and Publication of Results

There will be formal notification of internal audit results to the responsible departments, and iTrusChina will inform the subscribers in time of the potential security risks.

After the completion of the assessment done by the third-party auditing firm, the audit report will be provided to iTrusChina. After iTrusChina's rectification and the reassessment are completed, iTrusChina will publish the final audit results on the official website.

8.7 Other Assessments

According to the requirements of *Electronic Signature Law of the People's Republic of China*, *Measures for the Administration of Electronic Certification Services*, and *Regulations on Cryptographic Management of Electronic Certification Services*, etc., it is subject to certificate renewal and review by competent authorities every five years.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance and Renewal Fees

iTrusChina can charge the certificate subscriber based on the electronic certification services provided, and the specific fee standard is determined at discretion according to the regulations of the market and the management department. Within the range of the charging standard, i.e. no higher than the standard charge, iTrusChina has the right to introduce different charging strategies or preferential measures to different groups of subscribers according to the market conditions.

If the price specified in the agreement signed by iTrusChina with customer is inconsistent with the price announced by iTrusChina, the price in the agreement shall prevail.

9.1.2 Certificate Access Fees

During the validity period of the certificate, iTrusChina does not charge special fees for certificate access. If the user asks for special needs, extra fees may be needed to pay, which will be charged based on the negotiation of iTrusChina Marketing department with the user.

9.1.3 Revocation or Status Information Access Fees

iTrusChina should not charge any fee for the acquisition of CRL.

iTrusChina should not charge any fee for OCSP services.

9.1.4 Fees for Other Services

If iTrusChina provides the subscriber with certificate storage media and related services, iTrusChina will specify the price in the agreement signed with the subscriber or other entities.

9.1.5 Refund Policy

If the subscriber contract cannot be fulfilled or the subscriber certificate cannot be used due to iTrusChina, iTrusChina will return the related fee to the subscriber.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

iTrusChina should provide certificate subscribers with certificate usage support. If the user suffers losses during the use of the certificate due to iTrusChina, iTrusChina should provide indemnity to the certificate subscriber and the relying party (see Section 9.9 of this CP for details).

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

If iTrusChina violates the responsibilities stipulated in this CP, entities like certificate subscribers, relying parties, etc. may require iTrusChina to bear the liability for compromise (except for statutory or agreed liability exemptions).

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

In the electronic certification service provided by iTrusChina, the following information is treated as confidential information:

1）Audit records include information of local logs, server logs, archived logs, which are treated as confidential information by iTrusChina and can only be viewed by security auditors and service administrators, and cannot be published outside the company except for legal requirements.

2）Other personal and company information maintained by iTrusChina and registration authority should be kept confidential, and cannot be published except for legal requirements.

9.3.2 Information Not within the Scope of Confidential Information

iTrusChina treated the following information as not confidential information:

1）Certificates issued by iTrusChina and information in CRL.

2）Information in the certificate policy supported by iTrusChina and identified by CPS.

3）Information\published on iTrusChina's website to the public, and approved available for subscribers' usage only.

4）The confidentiality of iTrusChina's other information depends on special data items and applications.

9.3.3 Responsibility to Protect Confidential Information

CA, its RAs, subscribers and participants related to the certification service are all obliged to undertake the corresponding responsibility for protecting confidential information according to the regulations of this CP, and shall protect confidential information by effective technical means and management procedures.

When the owner of the confidential information, for some reason, requires iTrusChina to make public or disclose the confidential information that he or she owns, iTrusChina should meet the owner's requirements; meanwhile, iTrusChina will require the owner of the confidential information to authorize the application in writing to express the owner's willingness of publicity or disclosure. If this behaviour of disclosing confidential information involves any other party's liability for indemnification, iTrusChina shall not bear any loss related to or arising from the disclosure of confidential information. The owner of confidential information shall bear all liabilities for indemnification arising from or related to the disclosure of confidential information.

When iTrusChina is required to provide confidential information stipulated in this CP through legal procedures by any law, rule, court, or other public authority, iTrusChina should publish the relevant confidential information to the law enforcing agencies in accordance with requirements of laws, regulations and court judgments. iTrusChina assumes no responsibility. Such provision is not regarded as a breach of requirements or obligations on confidentiality.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

iTrusChina shall formulate a privacy protection plan to keep subscribers' personal information confidential.

9.4.2 Information Treated as Private

Information treated as privacy includes:

1）the valid documents number of the subscriber, such as the ID card number, the organization code.

2）the subscriber's phone number.

3）the subscriber's mailing address and home address.

4）the bank account number of the subscriber.

5）the agreement signed between subscriber with iTrusChina and iTrusChina's RA.

9.4.3 Information not Deemed Private

Information that is not deemed private information of the certificate subscriber includes, but is not limited to, the following information:

1）certificate and certificate status information.

2）subscriber's name, organization name, etc.

3）subscriber's gender, organization type, etc.

4）postcode of subscriber's mailing address.

5）subscriber's email.

6）information that subscriber requires to be in the certificate.

9.4.4 Responsibility to Protect Private Information

iTrusChina and its RAs have the responsibility and obligation to properly keep and protect the private information specified in Section 9.4.2 of this CP.

9.4.5 Notice and Consent to Use Private Information

iTrusChina will take appropriate steps to protect the personal privacy of certificate subscribers, and will adopt reliable security measures to protect the stored personal private information.

iTrusChina and its RAs should inform certificate subscribers in advance and obtain consent and authorization if they need to use private information of certificate subscribers beyond the agreed scope and purposes; without subscribers' consent and authorization, iTrusChina will not disclose subscribers' private information to any third party.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In accordance with laws, administrative laws and regulations, regulations, decisions, orders, etc., due to judicial actions or administrative enforcement needs with legal authorization, iTrusChina and its RAs may need to provide the relevant information to law enforcing agencies and administrative execution organs with subscribers knowing or not knowing. Even if this happens, iTrusChina and its RAs will protect subscriber's private information as much as possible.

9.4.7 Other Information Disclosure Circumstances

Disclosure of other information is subject to laws and subscriber agreements.

9.5 Intellectual Property Rights

iTrusChina enjoys and retains intellectual property rights like copyrights and patent rights of all the software, materials, data and information published to the public and provided by iTrusChina, as well as certificate issued by iTrusChina through various channels, such as websites.

iTrusChina enjoys the ownership, right of name, and benefit sharing right of the digital certificate system software, and has intellectual property rights for the issued certificates, certificate revocation lists and the information therein.

iTrusChina has intellectual property rights for this CP and related operation management work documents. According to the Mozilla Root Policy, Mozilla can use this CPS on the premise of complying with the CC BY 4.0 agreement .

The certificate subscriber has intellectual property rights for the certificate registration information and the trademarks, service marks, trade names and distinguished names contained in subscriber's certificate.

The key pair of the certificate is the intellectual property of the entity corresponding to the subject or entity owner in the certificate.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

iTrusChina makes following commitment during the process of providing electronic certification services:

1) The certificate issued to the subscriber meets all the substantive requirements of this CP.

2) Notify the certificate subscriber of any known event that will affect the validity and reliability of the certificate of the subscriber in nature.

3) The certificate will be revoked in time in accordance with the requirements of this CP.

4) If iTrusChina is not affiliated with a subscriber, iTrusChina and the subscriber are two parties of a legally effective and executable subscriber agreement, and the subscriber agreement meets the requirements of the Baseline Requirements issued by the CA/Browser Forum; if iTrusChina is the same entity or is associated with the subscriber, the applicant has approved the terms of use;

5) Establish and maintain a database that is open 24*7 for all current status information (effective or revoked) of all unexpired certificates.

After publicly issuance of the certificate, iTrusChina ensures that other subscriber information in the certificate is accurate except for the non-verified subscriber information.

iTrusChina is not responsible for assessing whether the certificate is used within the appropriate range, and the subscriber and the relying party ensure that the certificate is used for the appropriate purposes of use in accordance with the subscriber agreement and the relying party's agreement.

9.6.2 RA Representations and Warranties

The commitment of iTrusChina’s RA in the process of participating in the electronic certification service is as follows:

1) The registration process provided to the certificate subscriber fully complies with all the substantive requirements of this CP;

2) If a certificate is refused to issue, all fees paid will be refund to the certificate applicant immediately;

3) Verify that the applicant has the right to use or control the domain name and IP address which is listed in the certificate subject field and the Subject Alternative Name field (or, only for the domain name, has obtained the authorization of the owner of the right to use or control domain name);

4) Verify that the applicant or the applicant's representative has been authorized to apply for a certificate on behalf of the applicant;

5) Verify the accuracy of all the information contained in the certificate (except for organizationalUnitName information);

6) Take verification measures to reduce the possibility of misleading information contained in the certificate subject "organizationalUnitName";

7) Verify the identity of the applicant in accordance with the requirements of Section 3.2 of this CP;

8) RA will submit service applications for revocation and renewal, etc. to iTrusChina in time according to the regulations of CPS.

9.6.3 Subscriber Representations and Warranties

Once a subscriber accepts the certificate issued by iTrusChina, it is deemed to make the following commitment to iTrusChina, its RAs and the relevant parties trusting the certificate:

1) has known and accepted the responsibility clauses in the subscriber agreement of iTrusChina and all the terms and conditions in this CP.

2) Use the certificate private key for digital signature within the validity period of the certificate.

3) The information, materials provided and statements made by the subscribers for applying for a certificate are true, complete and accurate. In case of any change in the foregoing information, materials or statements, the subscriber shall notify RA in time in writing. The subscriber shall bear all the legal responsibilities on subscriber's own, if the subscriber intentionally or negligently provides false or falsified information, materials or statements, or the subscriber does not notify RA in time in writing after the provided information, materials and statements are changed.

4) If there is an agent, both the subscriber and the agent are jointly and severally liable. The subscriber is responsible for informing iTrusChina or its authorized RAs on any false statement or omission made by the agent.

5) Each signature made by the private key corresponding to the public key contained in the subscriber's certificate is the subscriber's own signature, and the certificate is a valid certificate (the certificate is not expired or revoked) when the signature is signed, and the private key of the certificate is accessed and used by the subscriber itself.

6) Once the certificate is accepted, it means that the subscriber knows and accepts all the terms and conditions in this CP, and knows and accepts the corresponding digital certificate subscribe agreement

7) Once the certificate is accepted, the subscriber shall assume the following responsibilities: always maintain control of its private key; use a trusted system; take safe and reasonable steps to prevent the loss, compromise, tampering, or unauthorized use of the private key, and if the subscriber knows or should know that the private key or password of the certificate has already or may have already been lost, compromised, tampered or used without authorization, the subscriber shall notify the parties concerned in time in writing and terminate using the certificate immediately.

8) Prohibited for rejecting any statements, changes, updates, upgrades, etc., published by iTrusChina, including but not limited to modifications of policies and specifications as well as additions and deletions of certificate services, etc.

9) The subscriber shall use certificate within the range specified in this CP and is used only for authorized or other legitimate use purposes and shall not be used in scenarios other than the purposes of use.

10) Regarding EV SSL certificates, subscribers have the responsibility and obligation to ensure that certificates are deployed only in the servers corresponding to the subject alternative name listed in the certificate.

9.6.4 Relying Party Representations and Warranties

The relying party claims and commits: it evaluates the suitability of trusting certificates in specific applications and does not trust certificates in applications other than the appropriate purposes of certificates. The commitment of the relying party in the process of participating in the electronic certification service is as follows:

1) Have read all rules and restrictions of this CP, corresponding CPS and the relying party agreement, and agree to the provisions of this CP on the limitation of iTrusChina's liability prior to any trust act.

2)Before trusting the certificate, evaluate the appropriateness of trust certificate in a specific application, understand the purpose of the use of the certificate, and confirm whether the use of the certificate is in accordance with the provisions of this CP within the specified range and period.

3) Verify the trust anchor of the certificate before trusting a certificate.

4) Confirm whether the certificate is revoked by querying CRL and/or OCSP before trusting a certificate.

5) In the event of negligence or other reasons that violate the terms of a reasonable check, the relying party is willing to compensate for the loss caused to iTrusChina and to bear the loss of its own or others.

6) Prohibited for rejecting any statements, changes, updates, upgrades published by iTrusChina, including but not limited to modifications of policies and specifications as well as additions and deletions of certificate services.

9.6.5 Representations and Warranties of Other Participants

Other participants engaged in electronic certification activities shall undertake to comply with all the regulations of this CP.

9.7 Disclaimers of Warranties

One of the following cases shall exempt iTrusChina from the liability to warranties, and iTrusChina does not bear any legal liability to any party, including but not limited to liability of compensation and liability of indemnity:

1) When applying for and using iTrusChina's digital certificate, subscribers have violated one of the following obligations:

- The subscriber is obliged to provide true, complete and accurate materials and information, and shall not provide false or invalid materials or information;
- The subscriber shall keep the digital certificate carrier issued by iTrusChina properly and protect the PIN code, and shall not leak the PIN code or deliver the digital certificate carrier to others at will;
- When a subscriber applies its own key or uses a digital certificate, the subscriber should use a reliable and secure system;
- When the subscriber knows that the confidentiality of the electronic signature has been compromised or may have been compromised, the subscriber should timely inform iTrusChina and the relevant parties and terminate the use of the electronic signature.
- When subscribers are using digital certificates, they must abide by the laws, regulations and administrative rules of the country. Digital certificates shall not be used for any other purpose beyond the range of use regulated by iTrusChina;

- The subscriber shall use the certificate within the valid period of the certificate; shall not use the digital certificate of which the confidentiality has been compromised or may have been compromised, expired, frozen or revoked;
- The subscriber is obliged to pay the service fees to iTrusChina on time as stipulated.

2) Digital certificate issuance delay, interruption, inability to issue, or suspension or termination of all or part of the certificate services caused due to force majeure; "force majeure" stipulated in this provision refers to an unforeseeable, unavoidable and insurmountable objective circumstance, including but not limited to:

- Natural phenomena or natural disasters, including earthquakes, volcanic eruptions, landslides, debris flows, avalanches, floods, tsunamis, typhoons and other natural phenomena;
- Social phenomena, social anomalies, or government acts, including new policies, laws and administrative regulations issued by government, or social anomalies such as war, strike, and riot.

3) Digital certificate issuance, delay, interruption, inability to issue, or suspension or termination of all or part of the certificate services caused by iTrusChina's technical failures such as equipment or network failure; reasons for "technical failures" stipulated in this provision include but are not limited to:

- Force majeure;
- Caused by associated units such as electricity, telecommunication and communication units;
- Hacker attack;
- iTrusChina's equipment or network failure.

4) iTrusChina has carefully followed digital certificate certification rules stipulated by national laws and regulations, yet there are still losses arising.

9.8 Limitations of Liability

Certificate subscribers and relying parties suffer losses in civil activities due to electronic certification services provided by iTrusChina, and iTrusChina will bear the limited liability of indemnification stipulated in Section 9.9 of this CP.

9.9 Indemnities

iTrusChina shall explain claims for indemnity in CPS.

9.10 Term and Termination

9.10.1 Term

The CP comes into effect at 0:00 on the effective date, and the previous version of CP becomes invalid at the same time; This CP becomes invalid on the day when the next version of CP becomes effective or when iTrusChina terminates the electronic certification service.

9.10.2 Termination

When iTrusChina terminates electronic certification service, this CP is terminated.

9.10.3 Effect of Termination and Survival

After the termination of this CP, its effect will be terminated at the same time, but the legal facts that occur before the date of termination, the provisions of the responsibility of the parties and the exemption of liability in this CP are still applicable, including, but not limited to, the contents of audit, confidential information, privacy protection, intellectual property, etc. in CPS, as well as limited liability clauses relating to indemnification, and are still valid after this CPS is terminated.

When some provisions in CPS, subscriber agreements, relying party agreements and other agreements become invalid due to some reason, such as content modifications or conflict with applicable laws, they do not affect the force of law of other provisions in the corresponding document.

9.11 Individual Notices and Communications with Participants

iTrusChina and its RAs, in the case of the necessary circumstances, such as the active revocation of subscriber certificates, the discovery that the subscriber uses the certificate for purposes other than those regulated purposes and has other behaviors violating the subscriber agreement, should individually notify the subscriber and the relying party by appropriate means, such as telephone, e-mail, letter, and fax, etc.

After the termination of this CP, iTrusChina should notify the parties concerned about the invalidation of the document.

9.12 Amendments

9.12.1 Procedure for Amendment

Authorized by iTrusChina's Security Policy Administration Committee, the CP compiling team reviews this CP at least once a year to ensure that it complies with national laws and regulations and meets the requirements of administration department and the competent authorities, meets relevant international standards, and meets the actual needs of the certification business development.

Regarding the amendment and update of this CP, the CP compiling team proposes an amendment report, and organizes the amendment after being approved by iTrusChina's Security Policy Administration Committee, and the revised CP will be officially published to the public after being approved by the Committee.

9.12.2 Notification Mechanism and Period

The revised CP will be published immediately on iTrusChina's official website upon approval. iTrusChina will notify the parties concerned in a reasonable period of time for amendments that need to be notified through e-mail, letter, media and other means. The reasonable time should ensure the least impact on the parties concerned.

9.12.3 Circumstances under Which Business Rules must be changed

Circumstances under which iTrusChina must change this CP include: the inconsistency between the relevant contents of the CP and the governing laws, and the specific changes or adjustments is required by national regulatory authorities on the certification service of iTrusChina.

9.13 Dispute Resolution Provisions

When there is a dispute among iTrusChina, the subscriber and the relying party, it should be resolved firstly through friendly negotiation in accordance with the agreement; if negotiation fails, it can be resolved through legal means.

9.14 Governing Law

This CP of iTrusChina is under the jurisdiction of the laws and regulations of the *Electronic Signature Law of the People's Republic of China, Measures for the Administration*

of Electronic Certification Services, and Measures for the Administration of Cipher Codes for Electronic Certification Services.

9.15 Compliance with Applicable Law

The implementation, interpretation and procedural validity of this CP are applicable to the law of the People's Republic of China, regardless of where entities like iTrusChina's certificate subscribers, relying parties are living and where iTrusChina's certificates are used. Laws of the People's Republic of China apply to any dispute with iTrusChina or its RAs concerning this CP.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The entire document structure of this CP includes 3 parts: title, contents and main body contents. The replacing contents of the contents and the main body contents after modification will completely replace all the previous parts and will be published on iTrusChina's website for public viewing.

9.16.2 Assignment

In accordance with the rights and obligations of the certification entities specified in this CP, iTrusChina declare that the parties concerned cannot assign by any means, without prior written consent of iTrusChina.

9.16.3 Severability

If any clause of the CP or its application is judged to be invalid or ineffective as a result of conflict with the law in the jurisdiction where iTrusChina is located, iTrusChina can modify any conflicting provision to the minimum extent necessary to make it continue to be valid and the remaining parts are not affected, and iTrusChina will disclose the modification in this section.

Prior to issuing a certificate under the modified requirement, iTrusChina will notify the CA/Browser Forum of the relevant information newly added to its CP and CPS by sending a message to question@cabforum.org and receiving confirmation that it has been posted to and is indexed in the Public Mailing List (https://cabforum.org/pipermail/ public/).

Any modification to iTrusChina practice enabled under this section must be discontinued if and when the law no longer applies, or the Baseline Requirements of the CA/B forum are modified to make it possible to comply with both BR and the law simultaneously. An appropriate change in practice, modification to iTrusChina's CP and CPS and a notice to the CA/B forum, as outlined above, must be made within 90 days.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

The CPS formulated under this CP shall include force majeure clauses to protect the interests of all parties.

9.17 Other Provisions

iTrusChina has the final interpretation right of this CP.