ITRUSCHINA™

GLOBAL-TRUST

CERTIFICATE POLICY

AND CERTIFICATION

PRACTICE STATEMENT

V 1.6.1

Effective Date: Apr 30, 2025

Version Description:

Version Control Table

Name & Version	Main Revision Description	Effective Date	Reviser
CPS V1.3	1) Specified the way to submit a certificate problem report; 2) Modified requirements for validation of IP address on section 3.2.2.5; 3) Minor changes on validation procedures. 4) The CPS first published in English.	May 9, 2019	CP/CPS team
CPS V1.3.1	1) Add Annex B root certificate information	Jul 1, 2019	CP/CPS team
CPS V1.4	2，According to the BR SC25, adjust methods 3.2.2.4.2 in this CPS 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
CPS V1.4.1	1 ， 5.2.2 Modified the management authority of cryptographic device from 2 out of 3 to 3 out of 5. 2 ， 6.2.2 Modified the Private Key Multiple -person Control from 2 out of 3 to 3 out of 5.	May 20, 2020	CP/CPS team

Name & Version	Main Revision Description	Effective Date	Reviser
	3，Validity period of subscriber certificates and verification data are adjusted to 398 days.		
CPS 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
CPS V1.4.3	1，Modified some descriptions of the authentication process in Annex A.	Dec 9, 2020	CP/CPS team
CPS V1.4.4	2，Modified some descriptions of the authentication process in Annex A. 2 ， Modified the name of this document.	Dec 19, 2020	CP/CPS team
CPS V1.4.5	1, Add description about demonstrate private key compromise.	May 1, 2021	CP/CPS team
CPS V1.4.6	1, Modified some descriptions .	Sep 15, 2021	CP/CPS team
CPS V1.4.7	1, Add description about EV SSL authentication process. .	October 10, 2021	CP/CPS team
CPS V1.4.8	1. Added the description of Adobe document signing certificates and time stamping certificates. 2. Make corresponding adjustments according to CAB Ballot SC45.	October27, 2021	CP/CPS team

Name & Version	Main Revision Description	Effective Date	Reviser
CPS V1.4.9	Modified some descriptions .	Mar 25, 2022	CP/CPS team
CPS V1.5	1. Modified the description of logs' types and retention in 5.4 and 5.5 base d on BR. 2. Added the description of revocation reasons in 7.2.2. 3. Change the revision time of CP from one year to 365 days. 4. Modified some other descriptions.	Mar 15, 2023	CP/CPS team
CPS V1.5.1	1. Add SCT extension according to the description in Section 7.1.2 of BR 2.0.0.	Aug 8 2023	CP/CPS team
CPS V1.5.2	1. Modified the descriptions of HSM and secret share media 2. Modified the update frequency of CRLs and OCSP responders	Nov 23, 2023	CP/CPS team
CPS V1.5.3	1. Modified iTrusChina CA Hierarchy in Section 1.1.3 2. Modified description of certificate extensions in Section 7.1.2 3. Modified some other descriptions	Dec 15, 2023	CP/CPS team
CPS V1.5.4	1. Added the description of domain validation in Section 3.2.2.4 2. Added the description of IP address validation in Section 3.2.2.5 3. Modified the description of wildcard domain validation	Mar 28, 2024	CP/CPS team

Name & Version	Main Revision Description	Effective Date	Reviser
	4. Modified the validity period of the certificate validation material 5. Added the description of precertificate revocation and SCT 6. Modified the description of certificate revocation request processing and revocation request grace period 7. Added the description of linting tools in Section 6.1.5 8. Modified the description of public key archival 9. Added the description of precertificate in Section 7.1.2		
CPS V1.5.5	Added information on the new ICA and new OID	Jul 10, 2024	CP/CPS team
CPS V1.5.6	1. Added information about the time stamping service and validation of TS cert. 2. Modified certain descriptions.	Aug 22, 2024	CP/CPS team
CPS V1.5.7	Modified some descriptions of TS cert	Sep 24, 2024	CP/CPS team
CP/CPS V1.6	1. Combined CP and CPS. 2. Modified certain descriptions.	Mar 24, 2025	CP/CPS team
CP/CPS V1.6.1	Modified the CRL issuance frequency of subscriber certificates	Apr 30, 2025	CP/CPS team

Contents

1. Introduction

1.1 Overview

1.1.1 Company Introduction

iTrusChina Co.,Ltd. (hereinafter referred to as "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, With internationally standardized capacity of operational, management and services， provides global electronic certification service for internet users with various needs on tele-communication and information security.

1.1.2 Certificate Policy and Certification Practice Statement

The *"Certificate Policy and Certification Practice Statement"* (CP/CPS for short) described in this document is the highest policy and practice rules for iTrusChina's SSL certificates, Document Signing certificates and Timestamp certificates, it applies to all the PKI participating entities of iTrusChina Global-Trust system. This CP/CPS clarifies how iTrusChina conducts electronic certification services, including service modes and processes of approving, issuing, managing, revoking and renewal certificates, as well as the corresponding service, legal and technical measures and safeguards for the participants of electronic certification activities to understand and follow.

This CP/CPS follows the framework requirements of RFC 3647, and its general provision structure conforms to the *Standards for Electronic Certification Practice Statement (Trial)* issued by the Ministry of Industry and Information Technology and during the formulation process, follow the requirements of laws and regulations of *Electronic Signature Law of the People's Republic of China*, *Measures for the Administration of Electronic Certification Services*, *Measures for the Administration of Cipher Codes for Electronic Certification Services*, etc.

This CP/CPS also complies with the latest version of *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server 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*（"NCSSR" for short） issued by CA/Browser Forum, *Adobe Approved Trust List Technical Requirements* ("AATL" for short） to issue and manage public trusted SSL certificates, Document Signing certificates and Time Stamping certificates. iTrusChina will notify the CA/B Forum If a court or government body in China with jurisdiction over the activities covered by the EV Guidelines determines that the performance of any mandatory requirement is illegal. iTrusChina regularly checks standards updated from CA/Browser Forum and continuously revises the CP/CPS according to the published version. If this CP/CPS and the terms in the relevant standards and specifications issued by CA/Browser Forum are inconsistent, the specifications issued by CA/Browser Forum will prevail.

1.1.3 iTrusChina CA Hierarchy

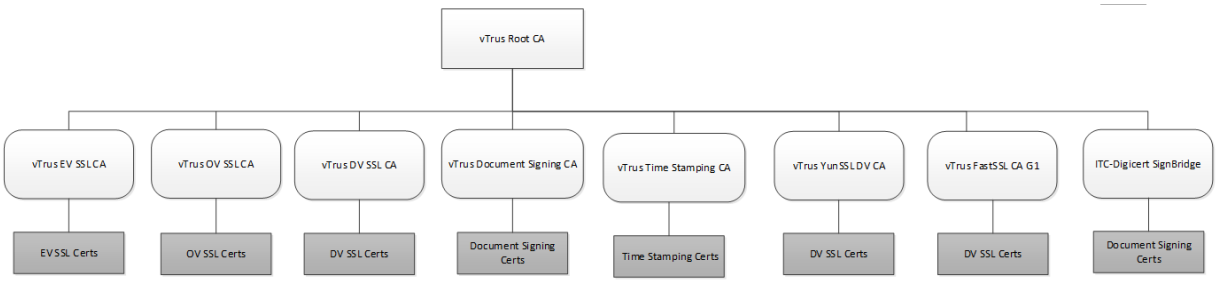
Currently, iTrusChina has 2 root CA certificates, vTrus Root CA Certificate (RSA) and vTrus ECC Root CA Certificate (ECC), with subordinate CA for each root CA to issue subscriber certificates. iTrusChina does not issue external subordinate CA certificates.

1) iTrusChina Root CA

The cryptographic algorithm of vTrus Root CA certificate is RSA, and the root key size is 4096-bit; this root CA has 8 subordinate CA certificates:

- vTrus EV SSL CA certificate with a key size of RSA 2048-bit issues EV SSL server certificate with a key size of RSA 2048-bit;
- vTrus OV SSL CA certificate with a key size of RSA 2048-bit issues an OV SSL server certificate with a key size of RSA 2048-bit;
- vTrus DV SSL CA certificate with a key size of RSA 2048-bit issues a DV SSL server certificate with a key size of RSA 2048-bit.
- vTrus YunSSL DV CA certificate with a key size of RSA 2048-bit issues a DV SSL server certificate with a key size of RSA 2048-bit.

- vTrus FastSSL CA G1 certificate with a key size of RSA 2048-bit issues a DV SSL server certificate with a key size of RSA 2048-bit.
- vTrus Document Signing CA certificate with a key size of RSA 2048-bit issues a Document Signing certificate with a key size of RSA 2048-bit.
- ITC-Digicert SignBridge certificate with a key size of RSA 2048-bit issues a Document Signing certificate with a key size of RSA 2048-bit.
- vTrus Time Stamping CA certificate with a key size of RSA 4096-bit issues a Time Stamping certificate with a key size of RSA 4096-bit.

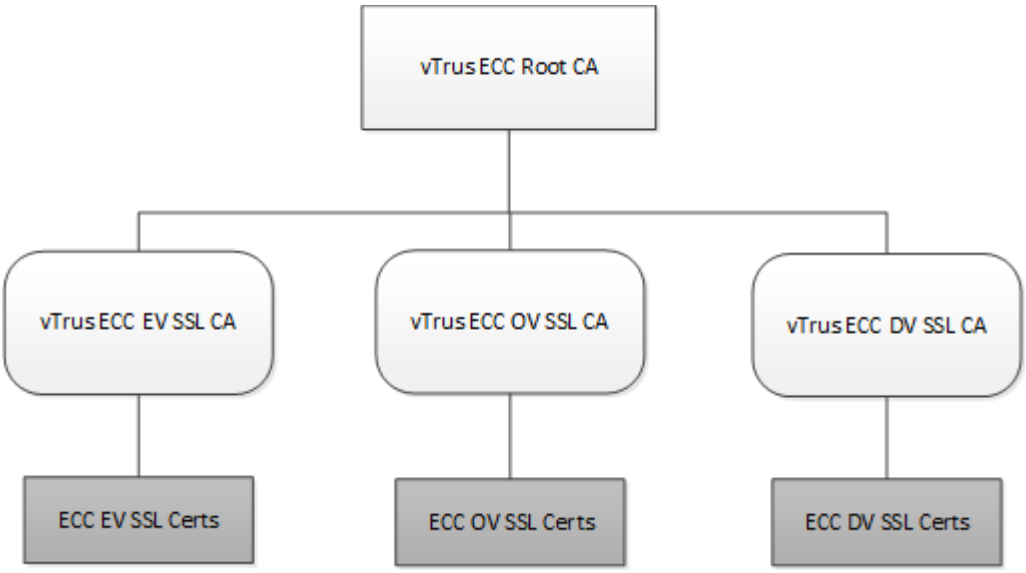


A Three-Level Root System Diagram of RSA

2) vTrus ECC Root CA

The cryptographic algorithm of vTrus ECC Root CA certificate is ECC, and the root key size is 384-bit, this root CA has 3 subordinate CA certificates:

- vTrus ECC EV SSL CA certificate with a key size of ECC 256-bit issues an EV SSL server certificate with a key size of ECC 256-bit;;
- vTrus ECC OV SSL CA certificate with a key size of ECC 256-bit issues an OV SSL server certificate with a key size of ECC 256-bit;;
- vTrus ECC DV SSL CA certificate with a key size of ECC 256-bit issues a DV SSL server certificate with a key size of ECC 256-bit;.



A Three-Level Root System Diagram of ECC

1.2 Document Name and Identification

This document is called *iTrusChina Global-Trust Certificate Policy and Certification Practice Statement* (iTrusChina's CP/CPS, or this CP/CPS for short), CP is short for Certificate Policy and CPS is short for "Certification Practice Statement". In this document, CP/CPS is equivalent to the name and the applicable name of the document defined in this section.

The OID registered by iTrusChina is 1.2.156.112535, and the OIDs allocated for various certificates in this CP/CPS are as follows:

1) EV SSL Certificate Policy Object Identifier: 1.2.156.112535.1.1.6.1;

2) OV SSL Certificate Policy Object Identifier: 1.2.156.112535.1.1.5.1;

3) DV SSL Certificate Policy Object Identifier: 1.2.156.112535.1.1.5.2.

4) Document Signing Certificate Policy Object Identifier: 1.2.156.112535.1.1.4；

5) Individual Document Signing Certificate Policy Object Identifier：1.2.156.112535.1.1.4.1；

6) Enterprise Document Signing Certificate Policy Object Identifier：1.2.156.112535.1.1.4.2；

7) Enterprise Document Signing Certificate (planning for designated project) Policy Object Identifier：1.2.156.112535.1.1.4.3;

8) Time Stamping Certificate Policy Object Identifier：1.2.156.112535.1.1.3.

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.

The Chinese version of this CP/CPS is issued. iTrusChina sincerely guarantees that there is no materially difference between the Chinese and English versions of the information.

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 is a major participant of electronic certification service by issuing digital certificates, providing digital certificate authentication service, and Time Stamping 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 fulfills responsibilities as a certificate subscriber.

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

1.3.4 The subscriber represents the unique entity bound to the public key in the SSL certificate and has ultimate control over the private key that uniquely corresponds to its certificate. The subscriber SHALL use the certificate within the scope of this CP/CPS and bears the agreed obligations of this CP/CPS.Relying Parties

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

Before the trust or use of a certificate, a relying party MUST verify the certificate's revocation information by querying the Certificate Revocation List (CRL) or using OCSP to query the certificate status. A relying party MUST perform reasonable check before trusting 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

The digital certificates issued by iTrusChina include SSL server certificates, PDF document signing certificates and time stamping certificates.

SSL 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 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 may decide to apply appropriate certificate types according to actual needs.

The document signing certificates issued by iTrusChina is used to ensure the authenticity, integrity and confidentiality of a document. According to the application type and authentication

method, it is divided into enterprise document signing certificates and individual document signing certificates.

The time stamping certificates issued by iTrusChina is used for time stamping data.

1.4.1.1 EV SSL Certificate

EV SSL certificate is short for Extended Validation SSL Certificate. EV SSL certificate can be used to verify control of the domain listed in the certificate and the identity of corporation who is using this certificate. All EV certificates issued by iTrusChina are confirmed after verification that the information contained in the certificate is true and effective and has passed appropriate and reliable identity and domain authentication procedures. EV SSL certificate can be used for encrypt network traffic between server and client, and verify the identity of the websites.

1.4.1.2 OV SSL Certificate

OV SSL Certificate (Organization Validation Certificate) is a standard SSL certificate that needs to verify the true identity of the website's affiliate. OV SSL certificate can be used for encrypt network traffic between server and client, and verify the identity of the websites.

1.4.1.3 DV SSL Certificate

DV SSL Certificate (Domain Validation SSL Certificate) is a simple SSL certificate that only verifies the control over website's domain name. DV SSL certificate only provides the encryption function of website connections.

1.4.1.4 Document Signing Certificate

Document Signing Certificates, which provide the function of signing PDF documents, comply with the AATL requirements. When the signed document is opened with Adobe Reader, Adobe Acrobat, or other software it can automatically obtain a trusted identity and display whether the signature is valid.

1.4.1.5 Time Stamping Certificate

Time Stamping Certificates provide the function of time stamping data.

1.4.2 Limited Certificate Uses

A digital 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/CPS are not protected by this CP/CPS.

1.4.3 Prohibited Certificate Uses

Certificates issued by iTrusChina is prohibited to be used under any circumstance 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/CPS, and the Committee is responsible for formulating, approving, releasing, implementing, updating and aborting this CP/CPS. 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/CPS version may be deemed to be approved.

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

1.5.2 Contact Person

iTrusChina implements strict version control over this CP/CPS and assigns specific department responsible for related issues. For any problem, suggestion or question, please contact us as follows:

If you need iTrusChina related policy documents, 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: +8610-50947500

Fax Number: +8610-50947517/50947516

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

Subscribers, relying parties, application software suppliers and other third parties can submit certificate problem reports, including key compromise, certificate misused, and incorrect issuance to iTrusChina. Please visit https://www.itrus. com.cn/repository and fill it out according to the instructions in the Certificate Problem Report, submit it online or send it to compliance@itrus.com.cn .

1.5.3 Person Determining CP/CPS Suitability

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

1.5.4 CPS Approval Procedures

This CP/CPS 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/CPS is officially published on the official website of iTrusChina.

This CP/CPS is revised every 365 days 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/CPS compiling team submits CP/CPS 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/CPS on iTrusChina official website.

All officially published versions of this CP/CPS will be uploaded to Common CA Database (CCADB) per the relevant requirements.

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
Security Policy Administration Committee	It refers to the supreme policy administration and supervision organization in the certification service system and the decisive organization for CP/CPS 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）	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements. 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）	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
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.
Digital Certificate	It refers to a digital 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 Responsibilitys

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.

The CP/CPS of iTrusChina are available through iTrusChina official website; 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.cn" as CAA query tags.

2.3 Time or Frequency of Publication

iTrusChina CP/CPS are available through Repository on a 7x24 basis.

iTrusChina publishes CP/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 Email or certificate service sites provided by iTrusChina, 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 InternationalizedDomain 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/CPS 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

iTrusChina does not verify an Applicant's right to use a trademark and does not resolve trademark disputes.

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 of Organization 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 (Uniform social credit 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.

3.2.2.1.1 Authentication of EV SSL subscriber identity

1) EV SSL certificate application requirements

The EV SSL certificate application can only be the domain name of a WEB server, IP address application is not accepted, and the domain name cannot contain wildcards.

2）Applicant's Legal existence and identity

iTrusChina verifies the Applicant's legal existence and identity directly with the incorporating agency or registration agency:

Verify the applicant's identity information, business address, and registered address by querying the applicant's social unified credit code ， Corporate Annual Report and business license.

3) Applicant's operational existence

i. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years.
ii. Relying on a Verified Professional Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

4) EV SSL certificate subject field requirements

The subject:organizationName (OID 2.5.4.10) field contains the applicant's full legal organization name authenticated by the method in 3.2.2.1;

The subject:businessCategory (OID: 2.5.4.15) field contains one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity"; When the

content in the subject:businessCategory (OID: 2.5.4.15) field is "Business Entity", the subject of the certificate is an individual business operator, then the certificate applicant must be the operator himself, and must be verified in a "face-to-face" (video) way ；

The subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1),
subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2),
subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3) field contains the jurisdiction level of the registration authority. iTrusChina has disclosed the values in these fields in the latest public verification data source on the official website;

The subject:serialNumber (OID: 2.5.4.5) field contains a unified social credit code. iTrusChina has disclosed the acceptable registration number format in this field in the latest public verification data source on the official website;

The EV SSL certificate issued by iTrusChina does not contain the OU field and does not contain a DBA.

5) Roles of applicants related to EV SSL

Applicants for the EV SSL certificate can only be organizations such as Government Entity，Business Entity，and Private Organization. The applicant organization must have the following roles:

Certificate Requester: the handling personnel of the applying unit;

Certificate Approver: the person in charge of the applicant unit;

Contract Signer: The signer of the application agreement.

The certificate application organization can authorize one or more people to complete all roles. iTrusChina will contact the applicant organization by calling (the company phone number obtained through reliable data sources in 3.2.2.7) to determine the Certificate Requester, Certificate Approver, and Contract Signer personnel name ,title and authorization. iTrusChina will use the same method to verify that the signature on the certificate application and subscriber agreement is true and valid.

6) Separation of duties for EV authentication

After all verification processes and procedures are completed, iTrusChina will have a person who is not responsible for collecting information to review all the information and documents collected to support the EV certificate application, and approve the issuance of the EV SSL certificate.

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 CPS 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

iTrusChina will verify the control over all domain names listed in a certificate. According to the requirements on the CAB Forum, iTrusChina does not issue a certificate for the internal name of the application, 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 DNS TXT Record Email Contact for the Authorization Domain Name 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 3.2.2.4.4 and 3.2.2.4.14 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)

3.2.2.4.4 Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555. （as per the domain name verification methods in 3.2.2.4.19 in BR）

3.2.2.4.5 Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application‐Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. （as per the domain name verification methods in 3.2.2.4.20 in BR）

Note: The above methods mentioned in 3.2.2.4.1 and 3.2.2.4.3 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. The methods mentioned in 3.2.2.4.1 and 3.2.2.4.3 are suitable for validating wildcard domain names.

3.2.2.5 Authentication for an IP Address

According to the requirements of CAB Forum, iTrusChina does not issue a certificate for the Reserved IP marked by IANA. For all IP address listed in a certificate, iTrusChina confirms the control over the IP by one of the 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).

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).

iTrusChina does not issue 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 controlled by the applicant.

iTrusChina will access to "ICANN DOMAINS" in Public Suffix List (PSL), and rejects certificate requests 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.

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 any 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.cn" are not contained in "issue" and "issuewild" tags, iTrusChina will not issue the corresponding certificate; When the certificate requests or issuances violate the security policy of iTrusChina or the FQDN holder， the tag "iodef" exists in CAA records, iTrusChina will not dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s).

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

iTrusChina uses the following authentication methods to verify personal information:

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 and address. iTrusChina will verify information through government agencies or third-party trusted data sources.

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

3.2.4 Non-verified Subscriber Information

The certificate issued by iTrusChina does not contain any non-verified information.

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 Verified Method of Communication 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/CPS 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 Requests

Among iTrusChina's certificate practices, certificate revocation requests may come from subscribers, relying parties, and application software suppliers. In addition, if iTrusChina deems it necessary (see the relevant circumstance described in 4.9.1.1 of this CP/CPS), 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 Enrollment Process and Responsibilities

The 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, the iTrusChina's CP/CPS, etc beforehand, especially contents related to range of application, rights, obligations and warranties of certificates.

The applicant shall submit 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/CPS.

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 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 SSL 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.

For OV SSL certificate, iTrusChina can reuse previous validations if iTrusChina obtained the data or document from a source specified under Section 3.2 of this CP/CPS or completed the validation no more than 825 days prior to issuing the Certificate. For validation of Domain Names and IP Addresses according to Section 3.2.2.4 and 3.2.2.5, iTrusChina can reuse data, document, or completed validation if they are obtained no more than 398 days prior to issuing the Certificate.

For EV SSL certificate, iTrusChina can reuse previous validation data or documents to verify the information of certificates if they are obtained no more than 398 days.

For DV SSL certificates, iTrusChina does not reuse domain verification data.

Before the issuance of the PDF document signing certificate, if iTrusChina obtains data or certification documents from the source specified in section 3.2 of this CP/CPS for no more than 3 years and the information has not changed, iTrusChina can reuse the data or verification documents to verify the information in Document Signing certificates.

4.2.2 Approval and Rejection of Certificate Applications

After completing the identification and authentication in Section 4.2.1 of this CP/CPS, iTrusChina can approve or reject the application according to the result of authentication. If an application is rejected, iTrusChina shall notify the certificate applicant in a proper manner within a reasonable time.

If iTrusChina believes that the issuance of a certificate may cause disputes, legal disputes or losses to iTrusChina, iTrusChina may also refuse the application of the certificate.

iTrusChina has the right to refuse to issue a certificate for an agency that is explicitly prohibited by laws and regulations, state government departments, industry regulators, or local governments from commercial activities or other public activities. In addition, if the personnel related to the certificate application are restricted by the laws and regulations, the state or local government, iTrusChina may not accept the EV certificate application that the personnel are involved.

4.2.2.1 Approval of Certificate Applications

iTrusChina may approve a certificate application if:

1) according to regulations in Section 3.2 of this CP/CPS, all necessary subscriber information has been successfully identified and authenticated;

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

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

4.2.2.2 Rejection of Certificate Applications

iTrusChina has the right to reject a certificate application if:

1) according to Section 3.2 of this CP/CPS, it cannot fulfil the identification and authentication of all necessary subscriber information.

2) the subscriber cannot provide necessary identity proof materials;

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

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

5) 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

iTrusChina starts processing the certificate application within a reasonable time of receipt of the certificate request. In the case that the application materials submitted by the client are complete, iTrusChina will complete the certificate application within 5 working days.

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 authenticity of the received certificate application has been verified by RA.

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.

For the issuance of SSL certificates，before apply for SCT（Signed Certificate Timestamps），iTrusChina will use linting tools to detect errors on precertificates to prevent the issuance of certificates that violate the Baseline Requirements of the CA/Browser Forum. iTrusChina will revoke incorrect precertificates.

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 any of 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 24 hours.

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 SSL 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/CPS.

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. Key pairs and certificates shall not be used for purposes other than the prescribed and approved purposes.

Subscribers shall protect their private keys from unauthorized use and shall not use expired or revoked certificates. Parties other than subscribers are not allowed to archive the private key of subscribers.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties should consider the overall circumstance and the loss risk before trusting a certificate.

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.

6) considering other information in this CP/CPS or elsewhere.

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/CPS.

4.6.3 Processing Certificate Renewal Requests

iTrusChina processes subscriber certificate renewal requests as new certificate issuance, please see the Section 4.2 of this CP/CPS.

4.6.4 Notification of New Certificate Issuance to Subscribers

The same as Section 4.3.2 of this CP/CPS.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificates

The same as Section 4.4.1 of this CP/CPS.

4.6.6 Publication of the Renewal Certificate by the CA

The same as Section 4.4.2 of this CP/CPS.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The same as Section 4.4.3 of this CP/CPS.

4.7 Certificate Re-Key

Certificate re-key is the process that the original issuer uses a new key pairs and the same subject Distinguish Name to issue a new certiificate.

4.7.1 Circumstance for Certificate Re-Key

The same as Section 3.3 of this CP/CPS.

4.7.2 Who may Request Certificate of a new Public Key

The same as Section 4.1.1 of this CP/CPS.

4.7.3 Processing Certificate Re-Keying Requests

iTrusChina processes subscriber certificate re-key requests as new certificate issuance, and will check whether the key has been replaced, please see Section 4.6.3 of this CP/CPS.

4.7.4 Notification of New Certificate Issuance to Subscribers

The same as Section 4.3.2 of this CP/CPS.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The same as Section 4.4.1 of this CP/CPS.

4.7.6 Publication of Re-Keyed Certificate by the CA

The same as Section 4.4.2 of this CP/CPS.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The same as Section 4.4.3 of this CP/CPS.

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 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

iTrusChina processes subscriber certificate modification requests as new certificate issuance, please see Section 4.2 of this CP/CPS.

4.8.4 Notification of New Certificate Issuance to Subscribers

The same as Section 4.3.2 of this CP/CPS.

4.8.5 Conduct Constituting Acceptance of Modified Certificates

The same as Section 4.4.1 of this CP/CPS.

4.8.6 Publication of the Modified Certificate by the CA

The same as Section 4.4.2 of this CP/CPS.

4.8.7 Notification of the Certificate Issuance by the CA to Other Entities

The same as Section 4.4.3 of this CP/CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstance for Certificate Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

iTrusChina will revoke the certificate within 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;

iTrusChina will revoke the certificate within 5 days if one or more of the following occurs:

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 CP/CPS of iTrusChina;

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 CP/CPS;

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 (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

16) the fulfillment of obligations in CP/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 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 certificate 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 is terminated unless it continues to maintain the CRL/OCSP repository;

9) this CP/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 revocation request 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/CPS, 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. Subscribers can apply for revocation through the contract published in iTrusChina website.

4.9.3.2 A Subscriber Is Forced to Revoke a Certificate

1) when iTrusChina has sufficient reason to believe that circumstances that will cause the enforced revocation of subscriber certificates in Section 4.9.1.1 of this CP/CPS, iTrusChina will apply for the revocation of the certificate through the internal process;

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;

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.

3) 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

Once a certificate revocation is necessary, the subscriber should submit a revocation request within 8 hours. If it exceeds 8 hours, iTrusChina will not be responsible for any losses arising from the subscriber's failure to timely request revocation.

4.9.5 Time Within which CA must Process the Revocation Requests

Within 24 hours upon the receipt of a certificate problem report, iTrusChina 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. iTrusChina publishes a new CRL within twenty‐four (24) hours after recording a Certificate as revoked. Subscriber CRLs are valid for up to 7 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 4 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.

Any subscribers or relying parties could send certificate problem reports to iTrusChina (compliance@itrus.com.cn), and provide evidences of key compromise in the email. Upon verification of the key compromise, iTrusChina will revoke all instances of that compromised key across all subscribers. If it cannot be verified that the key has indeed been compromised, iTrusChina will only revoke all certificates associated with that subscriber that contain that public key and will block issuance of future certificates with that key.

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, and it is provided using HTTP protocol.

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 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 located on the Floor 4, Building 4, Courtyard 7, Shangdi Street 8, Haidian District, Beijing. The establishment of iTrusChina's computer room and system is carried out according to the following criteria:

1) GB/T 25056-2010 *Certificate Certification System Cryptography and Related Technical Security Specifications of Information Security Technology*

2) State Cryptography Administration [2010] July *Construction Requirements of E-government Affairs and Electronic Certification Infrastructure*

3) GB50174-2008 *Design Code for Electronic Information System Machine Room*

4) GB6650-86: *Technical Requirements for Raised Floor in Computer Room*

5) GB9361－2011 *Safety Requirements on Computer Station Site*

6) GB2887-2011 *General Specification for Computer Site*

7) GB50222-95 *Code for Fire Protection in Interior Decoration Design of Buildings*

8) GB50016 - 2014 *Code for Fire Protection of Architectural Design*

9) GB50116- 2013 *Design Code for Automatic Fire Alarm System*

10) GB50057－2010 *Design Code for Building Lightning Protection*

11) GB5054-2011 *Design Code for Low-Voltage Distribution*

12) GBJ19－2003 *Design Code for Heating, Ventilation and Air Conditioning*

13) YD/T754-95 *General Rule for Electrostatic Protection of Communication Room*

5.1.1.1 Public Area

The entrance, office area, auxiliary and support area of iTrusChina's site belong to the public area, and the access control measures are used to control the entry and exit by using identification card.

5.1.1.2 Service Area

The service area is the workspace of RA operators and managers. It requires both identification card and fingerprint identification at the same time for the access. There shall be log record for personnel's entry and exit of service area.

5.1.1.3 Management Area

The management area is the CA operation & management area, and the system monitoring room, the security monitoring room and the distribution room, etc. all belong to this area. This area requires identification card and fingerprint identification for the access.

5.1.1.4 Core Area

The certificate certification system, the cryptographic devices and other related cryptographic facilities are stored in the area, wherein the CA server, the database system, and the cryptographic devices are located in the shielding machine room of the core area.

The core area requires identification card and fingerprint identification for the access; it requires two trusted personnel in the shielding machine room using identification card and fingerprint identification at the same time for the access to ensure that a single person cannot perform sensitive operations in the shielded area.

5.1.2 Physical Access

iTrusChina's access control system in the service area, the management area and the core area can realize the entry and exit control of all areas, with the following functions:

- The access control of each door is controlled by means of identification card and fingerprint identification;
- There are log records for the entry and exit of every door;
- Doors of the service area, the management area and the core area are all equipped with forcible entry alarm and overtime alarm;
- The whole access control system is connected to UPS, and emergency power supply is provided by UPS at the time of power interruption.

The whole area is also equipped with video surveillance system, which carries out continuous video recording of important passages inside and outside the site for 7*24 hours. All video materials should be kept for at least 12 months for queries.

5.1.3 Power and Air Conditioning

iTrusChina has a safe and reliable power supply system and an electric power reserve system to ensure the normal power supply for 7*24 hours and to provide normal services in the case of power supply interruptions in the power supply system. In addition, iTrusChina also has a heating /ventilation /air conditioning system to control the temperature and humidity in the operation facilities.

iTrusChina's machine room uses an uninterruptible power supply system UPS, which can provide power supply for at least 8 hours. Anti-static precautions are adopted in the computer room to realize the potential bonding and grounding of cabinets, servers and network equipment, etc.

The air conditioner in the computer room adopts air-cooled condenser set, and the outdoor air-cooled condenser unit is placed on the top floor. The interior design temperature of the machine room is 23 + 2 C.

5.1.4 Water Exposures

The water leakage alarm system is deployed in iTrusChina's machine room. Once flood occurs, the system will immediately give an alarm to notify the relevant personnel to take emergency measures.

5.1.5 Fire Prevention and Protection

Smoke and temperature fire detectors are used in all areas of iTrusChina's machine room, and the automatic fire alarm system and the gas automatic fire extinguishing system have been installed. The system has two starting modes, automatic and manual operation.

In the automatic state, when the fire occurs in the protection area, the fire alarm controller sends the linkage signal immediately after receiving the two independent fire alarm signals in the protection area. After 30-second time delay, the fire alarm controls the output signal and starts the fire extinguishing system. At the same time, the alarm controller receives the feedback signal of the pressure signal device, and the door lights inside the protection area turn bright to avoid personnel straying.

When there are often people working in the protection area, the automatic state of the system can be switched to the manual state through the manual /automatic transfer switch outside the door of the protection area. In the case of ringing a fire alarm in the protection area, the alarm controller only sends out the alarm signal and does not output the action signal. The operator on duty confirms the fire alarm, presses the control panel or breaks the emergency start button outside the protection area, and it can immediately start the system and discharge the gas extinguishing agent.

In addition, according to the relevant national requirements on fire protection, iTrusChina has set up emergency exits in the management area. There are fire exit doors at emergency exits, while

there is no opening device outside these doors, and only from the inside can open these doors. Emergency exits have video surveillance devices for real-time monitoring. When a fire exit door is opened, the surveillance system will ring an alarm to notify personnel on duty.

5.1.6 Media Storage

iTrusChina keeps the media storing software and data, archiving, auditing, or backup information in security facilities. These facilities are protected by appropriate physical and logical access control, allowing only the access of the authorized personnel and preventing these media from accidental compromise (such as water, fire and electromagnetism).

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/CPS, 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 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 3 of 5 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 requires the participation of at least 2 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

To ensure the system security, iTrusChina implements the strategy 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, diploma, 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) BR and EV Guidelines compliance training.

5.3.4 Retraining Frequency and Requirements

Those who act as trusted roles or other important roles receive a training organized by iTrusChina at least once a year. Those who are related to the certification system operation receive relevant skill and knowledge training at least once a year. In addition, iTrusChina will irregularly require the personnel to continue the training according to the requirements of system upgrades and configuration modifications, etc.

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

iTrusChina doesn't hire external personnel engaged in the work related to certificate validation for now.

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;
- Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
- 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;
- Generation of Certificate Revocation Lists; and
- Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).

- Security events, including:

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- Installation, update and removal of software on a Certificate System;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

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; and
- Description of the entry.

5.4.2 Frequency of Processing Log

iTrusChina checks and summarizes the system's automatic log and operators' manual records once a month.

iTrusChina tracks and handles the system security log once a month to check violations of policies and other major 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 certificate requests and certificate authentication, verification, issuance and revocation shall be retained for at least 5 years after the certificate expires; other audit logs shall be kept for at least 2 years.

5.4.4 Protection of Audit Log

iTrusChina's system log is backed up in the log server, manual electronic records are backed up in SVN, and manual paper records are archived and stored in the management area.

iTrusChina has taken physical and logical access control methods to ensure that only the authorized personnel can approach these review records and strictly prohibit unauthorized access, reading, alteration and deletion.

5.4.5 Audit Log Backup Procedures

iTrusChina's system log is backed up to the log server in real time, and to the different places daily.

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 conducts vulnerability scanning work every 3 months and conducts a penetration test every year, and when there is a significant modification in the system or when receiving a request from CA/B, a vulnerability scanning or penetration test will also be conduct . According to security events found by the audit, iTrusChina will conduct the annual security vulnerability assessment of the system, physical sites, operation management, etc., and take measures to reduce the operational risk based on the assessment report.

5.5 Records Archival

5.5.1 Types of Records Archived

iTrusChina archives the following types of records:

1) Documentation related to the security of their Certificate Systems;

2) Documentation related to their verification, issuance, and revocation of certificate requests and Certificates;

3) CP, CPSand CP/CPS;

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

5) Various external and internal evaluation documents.

5.5.2 Retention Period for Archive

Archived audit logs (as set forth in Section 5.5.1) SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

5.5.3 Protection of Archive

iTrusChina has secure physical and logical protection measures and strict management procedures for various electronic and paper filing documents, ensuring that the archived

documents will not be compromised and preventing unauthorized access, alteration, deletion or other tampering behaviors.

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.

For written archive materials, backup is not required, yet strict measures are required to protect their security and prevent deletion, alteration, etc. of archives and their backups.

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

For system-generated electronic records, they are synchronized to the log server in real time and backed up to the off-site every day

For electronic records, the SVN server completes the collection and backup work.

For written archive materials, they are collected and archived into the management area.

5.5.7 Procedures to Obtain and Verify Archive Information

iTrusChina takes physical and logical 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

The end time of any certificate issued by iTrusChina's root certificate , including CA certificate and subscriber certificate, does not exceed the end time of the root certificate, and the end time of any subscriber certificate issued by CA certificate does not exceed the end time of CA certificate.

When the lifetime of the key pair that corresponds to the CA certificate exceeds the maximum life cycle specified in this CP/CPS, iTrusChina will start the key renewal process and replace the already expired CA key pair. For CA key changeover, iTrusChina will notify subscribers and other relevant parties in advance to avoid possible disruption of the CA services.

The key changeover of iTrusChina is carried out in the following ways:

1) the higher CA will stop issuing a new subordinate CA certificate ("the date of stopping issuance") before the expiration time of its private key is less than the lifetime of the subordinate CA key.

2) generate a new key pair and issue a new higher CA certificate.

3) after "the date of stopping certificate issuance", a new CA key will be adopted for issuing certificates for the approved subordinate CA or subscriber certificate request.

4) the higher CA continues to use the original CA private key to issue CRL until the last certificate issued by the original private key expires.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

iTrusChina has stipulated the corresponding incident and compromise handling procedures, and formulated various emergency response plans, including, but not limited to:

- The emergency plan of the power system;
- Fire emergency plan;
- Network and information system emergency plan;
- Key emergency plan, etc.

Staff of related posts will conduct regular emergency drills in accordance with relevant systems and emergency plans.

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

iTrusChina has backed up the resources, software and/or data of the service system and other important systems, and has developed the corresponding emergency handling process. In case of network failure, system and software compromise, database failure, etc., or a disaster caused by

force majeure, iTrusChina will implement the recovery 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/CPS.

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/CPS.

3) When the private key of iTrusChina 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

Once a major disaster occurs in the physical site, iTrusChina will resume the operation of CA system within 72 hours according to the business continuity plan, enabling it to provide certificate query and revocation services for subscribers; within 5 working days, iTrusChina will resume the certificate validation services and allow subscribers to apply for new certificates.

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 uses the HSMs complying with FIPS140-2 Level 3 specifications for CA key generation, management, storage, backup and recovery.

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 device. iTrusChina will reject the application if it finds that the subscriber is using a Debian weak key.

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

The public key of iTrusChina is included in the root CA certificate and the subordinate CA certificate issued by iTrusChina. The subscriber and relying parties can download the certificates from iTrusChina's certificate service site.

6.1.5 Algorithm type and Key Sizes

iTrusChina uses the keys with the following specifications：

Root CA Certificates：

digest algorithm：SHA256 and SHA384

RSA modulus size：4096

ECC modulus size：384

Subordinate CA Certificates：

digest algorithm：SHA256 and SHA384

RSA modulus size：2048 and 4096

ECC modulus size：256

Subscriber Certificates：

digest algorithm：SHA256

RSA modulus size：2048 and 4096

ECC modulus size：256.

iTrusChina uses the x509lint, zlint, and pkilint linting tools to ensure that the algorithm type and key length comply with the Baseline Requirements of the CA/Browser Forum.

iTrusChina will adjust the algorithm type and the key size according to the latest requirements of BR.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall be generated by using the cryptographic hardware and media complying with FIPS140-2 specifications.

Regarding the parameter quality check, since keys are generated and stored using the cryptographic hardware and media complying with FIPS140-2 specifications , 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.

The root CA key is generally used to issue the following certificates and CRL:

1) self-signed certificate representing the root CA;

2) subordinate CA certificate and cross certificate;

3) the CRL (ARL) of the root CA and the subordinate CA;

4) PKI system function certificates for specific purposes (such as OCSP certificates).

The subordinate CA key is generally used to issue the following certificates and CRL:

1) subscriber certificate;

2) time stamping certificate;

3) PKI system function certificate with specific purposes (e.g. OCSP certificate);

4) subscriber CRL.

The subscriber's key can be used to provide security services, such as information encryption and signature, etc.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

iTrusChina keys are generated using the HSMs complying with FIPS140-2 Level 3 specifications.

The process of CA key pair generation is completed by special key managers and several trusted employees of iTrusChina in iTrusChina's shielding computer room in accordance with

iTrusChina Key Generation Regulation. iTrusChina Key Generation Regulation stipulates the process control of CA key generation and relevant participants.

The cryptographic modules using to generate and store subscriber key pairs comply with FIPS140-2 Level 2 or higher specifications. The subscriber should protect and keep the cryptographic module to prevent the theft, loss, compromise and unauthorized use.

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

The generation, backup and recovery, etc. of all kinds of CA private keys of iTrusChina adopts a multi-person control mechanism. This mechanism is realized by splitting management jurisdiction of the cryptographic device through selecting three out of five, i.e. the management jurisdiction of the private key is dispersed in five different media (called secret split share, or secret split) to five trusted roles (called secret shareholders), and they save in internal safe boxes of iTrusChina. Only under the circumstance that at least three of them are present and permit, insert the administrator media and enter the PIN code can perform the operations of backup or recovery on the private key. The splits called secret shares is stored in the safe box in the shielding machine room when it is not used.

The activation of CA private keys of iTrusChina needs user jurisdiction media which have operator authority and are held by the key manager. The media are kept in the safe box in the shielding machine room until it's used to activated CA private keys.

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

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 media 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); another is to generate a cloning device and

administrator media 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).

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/CPS.

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

iTrusChina's key pair is generated, saved and used on the hardware cryptographic module. In addition, in order to achieve recovery, iTrusChina backs up the CA key according to the operation specification provided by the cryptographic device manufacturer. Besides, iTrusChina also has strict key management process to control the replication of CA key pair. All these measures have effectively prevented the loss, theft, alteration, unauthorized disclosure, and unauthorized use of CA private key.

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 are stored on the hardware cryptographic module complying with FIPS140-2 Level 3 specifications , and the use of private keys are also 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 USB Key), the document Signing certificate must be kept in a secure medium that meets FIPS 140-2 security specifications or a corresponding level, 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's private keys are stored on the hardware cryptographic module, and the activation is conducted by operation authority according to Section 6.2.2 of this CP/CPS. When the CA private key (in the online or offline cryptographic module) is needed for activating, the key manager in the company of Security management personnel obtains the user jurisdiction media, and then by the witness of System maintenance personnel accomplishes 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

After the life cycle of iTrusChina's private key ends, iTrusChina will continue to keep the CA private key in a backup hardware cryptographic module and archive it, and the other CA private key backups are safely destroyed. Meanwhile, all PIN codes and media, etc. for activating the private key must be destroyed. The archived CA private key must be destroyed safely under the circumstance of several trusted persons participating after its archive period ends. The destruction of the CA private key will ensure that the CA private key is completely deleted from the hardware cryptographic module without leaving any residual information.

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

See Section 6.2.1 of this CP/CPS for details.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

iTrusChina archives certificates by storing them in the database and making offsite backup, retention time is the same as retention time of the data in database.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period of the subordinate CA certificate is no more than 25 years, and the subscriber SSL certificate is valid for a maximum of 397 days.

The maximum validity period of the document signing certificate is no more than 3 years.

The validity period of the time-stamped certificate does not exceed 135 months.

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 iTrusChina's private key is generated by encryption device according to the operation specification provided by the encryption device manufacturer.

If the activation data of the subscriber certificate's private key is a password, the password must:

- contain at least 8 characters or numbers;

- contain at least one character and one number;
- cannot contain many same characters;
- cannot be the same as the name of the operator;
- cannot contain long substrings in user name information.

iTrusChina also recommends that subscribers use dual-factor mechanisms (e.g. hardware + password, biometric device + password, etc.) to control the activation of the private key.

6.4.2 Activation Data Protection

The activation data of the CA private key is held by different trusted personnel, and stored in their separate safe boxes in iTrusChina's shielding machine room.

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

Secret splitting media saving the activation data of the CA private key of iTrusChina certification authority and the private key of the operating device certificate are usually kept in the shielding machine room of iTrusChina, which cannot be taken out or transmitted. In case that it does need to be transmitted in some special circumstances, the transmission process must be carried out under the supervision of two trusted personnel of iTrusChina.

Normally, the private key activation data of subscriber's certificate is generated and kept by the subscriber's own, and should not be transmitted to other personnel. If the private key activation data needs to be transmitted for special reasons, the subscriber should protect them from loss, theft, alteration, unauthorized disclosure, or unauthorized use during the transmission.

The life cycle of activation data for subscribers applying for certificates is recommended as follows:

1. The subscriber's password for the application certificate becomes invalid after the application is successful.

2. Regarding the password used to protect the private key or secret splitting media, it is suggested that the subscriber should change it at any time according to the needs of the service application, and the subscriber should change it after the period of use exceeds 3 months.

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 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.

A strict dual-factor verification mechanism is implemented for every trusted person with system (including CA system, RA system) service operating authority, i.e. to use the login mode of double factors, user name, password and digital certificate at the same time.

System operation and maintenance personnel perform operations through the bastion host login system to ensure that CA software and data files are safe and reliable and will not undergo 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 controls the work of bring the certification system online by changing the internal control process, and requires the operation and maintenance personnel to strictly follow the approval and on line process execution, in order to assure the security and availability of the system:

1) The developed system must be strictly and successfully tested in the test environment before applying for the deployment in the production environment;

2) When applying for the deployment, changelog, test reports and deployment instructions, etc. should be provided;

3) The process of approval shall be execution according to the specification before deploying and going online;

4) Effective online backup shall be conducted before changing the deployment;

5) After changing the deployment, it should be tested immediately, and can provide external service only after passing the test.

iTrusChina has developed 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 has formulated various security policies, management regulations and processes for the safety management of the certification system.

The information security management of the certification system strictly follows 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 regularly performs security check on the system to identify whether the devices are being invaded, whether there are security vulnerabilities, etc.

6.6.3 Life Cycle Security Controls

iTrusChina controls 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 adopts 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 contain time and date information, and these time and date information are 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 is the national trusted standard time.

iTrusChina provides a time stamping service compliant with RFC 3161, issuing trusted time stamping tokens for the signatures on PDF documents. Our time stamping service uses a trustworthy source of time. The private key for time stamping certificate is generated and stored in HSMs complying with FIPS140-2 Level 3 specifications.

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

For the contents and extensions of the certificate issued by iTrusChina, please refer to the table below:

	root certificate	subordinate certificate	subscriber certificate	precertificate
Version	X.509 V3	X.509 V3	X.509 V3	X.509 V3
Signature Algorithm	SHA256RSA SHA384ECDSA	SHA256RSA SHA256ECDSA SHA384ECDSA	SHA256RSA SHA256ECDSA	SHA256RSA SHA256ECDSA
Subject	used for identifying X.500 DN name of the CA issuing certificates, including country, organization, department and common name	used for identifying X.500 DN name of the CA issuing certificates, including country, organization, department and common name	DV SSL certificate: including common name; OV SSL certificate: including country, organization and common name. EV SSL certificate: Including country, organization,	byte - for - byte identical to the subject field final certificate

			common name, registration number, physical address, registered address, be consistent with Section 9.2 in EVGL in CAB Forum, and does not include any subject attributes except as specified in section 9.2 of the EV Guidelines. Document Signing certificate and Time Stamping certificate: including country, organization and common name.	
Key Size	4096bits RSA	2048bits RSA(SSL and Document Signing CA) 4096bits RSA(Time Stamping CA)	2048bits RSA SSL and Document Signing certificate) 4096bits RSA(Time Stamping certificate)	2048bits RSA SSL certificate)
	384bits(P-384) ECC	256bits(P-256) ECC	256bits(P-256) ECC	256bits(P-256) ECC
Basic Constraint	The basic constraint extension of CA certificate is set to	The basic constraint extension of CA certificate is set to be	The basic constraint extension of subscriber certificate is set to be End-	The basic constraint extension of subscriber certificate is set to be End-

	be CA. This extension must be marked critical.	CA. This extension must be marked critical.	Entity. This extension must be marked critical.	Entity. This extension must be marked critical.
Extended Key Usage	N/A	If iTrusChina creates an intermediate CA certificate after 2019.1.1, this extension must be included SSL certificate ICA： serverAuth (1.3.6.1.5.5.7.3.1) clientAuth (1.3.6.1.5.5.7.3.2) Document Signing ICA: clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) Time Stamping ICA: timestamping (1.3.6.1.5.5.7.3.8)	SSL certificate： serverAuth (1.3.6.1.5.5.7.3.1) clientAuth (1.3.6.1.5.5.7.3.2) Document Signing certificate: clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) Time Stamping certificate: timestamping (1.3.6.1.5.5.7.3.8)	SSL certificate： serverAuth (1.3.6.1.5.5.7.3.1) clientAuth (1.3.6.1.5.5.7.3.2)
Certificate Policy	N/A	including the policy identifier specified by the issuer and the policy identifier reserved by CA/B Forum. including the CPS publish address of the issuer CA	including the policy identifier specified by the issuer and the policy identifier reserved by CA/B Forum. including the CPS	including the policy identifier specified by the issuer and the policy identifier reserved by CA/B Forum. including the CPS

			publish address of the issuer CA	publish address of the issuer CA
CRL Distribution Point	N/A	CRL distribution point extension specified by iTrusChina, and the relying party can download CRL according to the URL provided by the extension	CRL distribution point extension specified by iTrusChina, and the relying party can download CRL according to the URL provided by the extension	CRL distribution point extension specified by iTrusChina, and the relying party can download CRL according to the URL provided by the extension
Authority Key Identifier	N/A	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate
Subject Key Identifier	The subject key identifier extension provides a means of identifying certificates that contain a particular public key	The subject key identifier extension provides a means of identifying certificates that contain a particular public key	The subject key identifier extension provides a means of identifying certificates that contain a particular public key	The subject key identifier extension provides a means of identifying certificates that contain a particular public key

Authority Information Access	N/A	Including the OCSP responderof issuer.(accessMethod = 1.3.6.1.5.5.7.48.1) Including the access URL of issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2).	Including the OCSP responder of issuer. (accessMethod = 1.3.6.1.5.5.7.48.1). Including the access URL of issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2).	Including the OCSP responder of issuer. (accessMethod = 1.3.6.1.5.5.7.48.1). Including the access URL of issuer certificate. (accessMethod = 1.3.6.1.5.5.7.48.2).
SCT list	N/A	N/A	Including certificate transparency version number, certificate transparency log server ID, signature time of the certificate transparency log system, signature algorithm of the certificate transparency log data, and signature data of the certificate transparency log. For subscriber certificates, this extension is mandatory.	N/A

Precertificate Poison	N/A	N/A	N/A	OID： 1.3.6.1.4.1.11129.2.4.3 This extension must be marked critical
Key Usage	Key usage specifies the purposes of the certified public key. This extension must be marked critical.	Key usage specifies the purposes of the certified public key. This extension must be marked critical.	For the subscriber certificate, this extension is optional. For RSA certificates, the key usage is Digital Signature, Key Encipherment (a0), for ECC certificates, the key usage is Digital Signature (80). This extension must be marked critical. For Document Signing certificates，the key usage is Digital Signature； For Time Stamping certificates，the key usage is Digital Signature (80)	For precertificate, this extension is optional. For RSA certificates, the key usage is Digital Signature, Key Encipherment (a0), for ECC certificates, the key usage is Digital Signature (80). This extension must be marked critical.
SubAltName	N/A	N/A	SSL certificate: dNSName: either a FQDN or Wildcard Domain Name;	SSL certificate: dNSName: either a FQDN or Wildcard Domain Name; or iPAddress

			or iPAddress	
NotBefore	Date and Time valid from, use UTC/GMT+08:00	Date and Time valid from, use UTC/GMT+08:00	Date and Time valid from, use UTC/GMT+08:00	Date and Time valid from, use UTC/GMT+08:00
NotAfter	Date and Time valid to, use UTC/GMT+08:00	Date and Time valid to, use UTC/GMT+08:00	Date and Time valid to, use UTC/GMT+08:00	Date and Time valid from, use UTC/GMT+08:00

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 and the requirements in Section 7.1.4 of CA/B Forum Baseline Requirements.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The Certificate Policy Object Identifier is the same as Section 1.2 of this CP/CPS.

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 issuer is composed of the state, province, city, organization, department and common 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 CRL to indicate the reason for revocation.

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

  Code 1, keyCompromise, the key of the certificate has been or is suspected to be compromised

  Code 2, cACompromise, CA's private key has been or is suspected to be compromised

  Code 3, affiliationChanged, if verified information in the certificate has changed

  Code 4, superseded, replaced by new ones

  Code 5, cessationOfOperation, if the website with the certificate is shut down prior to the expiration of the certificate, or if the subscriber no longer owns or controls the domain name in the certificate

  Code 9, privilegeWithdrawn, revocation by CA due to non-compliance reasons

When the CRLReason code is not one of the above, the reasonCode extension will not be provided.

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.

7.3.3 OCSP Request and Response Processing

OCSP request contains the following data: protocol version, service request, target certificate

identitifier, and optional extensions, etc.

After receiving a request, the OCSP server conducts the following detections when responding:

- the message is well formatted
- The responder is configured to provide the request service.

The request includes the information needed by the responder server, and if any one of the prerequisites is not satisfied, the OCSP server will generate an error message; otherwise, return a definite reply.

All definite replies are digitally signed by iTrusChina OCSP signing certificate. The main reply status includes: the certificate is valid, revoked, unknown. The reply information is composed of the following parts：

- Version of the response syntax
- Identifier of the responder server
- Response to the request certificate
- Time when the response was generated
- Optional extensions
- The object identifier of signature algorithm
- The signature of the hashed reply information

If an error occurs, the OCSP responder server will return an error message which does not contain the signature of iTrusChina OCSP certificate. Error information may include:

- Request with incorrect formatting (malformedRequest)
- Internal error (internalError)
- Please try again later (trylater)
- Require signature (sigRequired)
- Unauthorized (unauthorized)

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 CCADB Self-Assessment according to CA/Browser Forum CCADB policy.

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 WebTruststandards .

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, honored 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 standards, 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 does not charge any fee for the acquisition of CRL.
iTrusChina does 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/CPS for details).

iTrusChina decides its insurance strategy based on its business development and the business development of Chinese insurance companies. For the EV certificate, iTrusChina has passed the financial audit of a third-party audit company, and has reserved the relevant insurance amount for the planned EV customers.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

The end entity of the electronic certification service warranty provided by iTrusChina is the certificate subscriber and the certificate relying party.

The end entity may require iTrusChina to bear the corresponding liability (except for statutory or agreed exemption) in accordance with the provisions of this CP/CPS or the effective legal instruments (such as judgment, arbitral award, etc.).

If the end entity plans to lodge a claim with iTrusChina on the loss caused within the valid period of the certificate, the end entity should submit a claim application in written within three years from the date of knowing or should know the occurrence of the loss; the claim becomes invalid after the period of three years.

iTrusChina bears the limited liability of indemnification to the end entity in accordance with Section 9.9 of this CP/CPS.

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 CP/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

iTrusChina has the responsibility and obligation to properly keep and protect the confidential information specified in Section 9.3.1 of this CP/CPS.

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/CPS, 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 behavior 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/CPS through legal procedures by any law, rule, court, or other public authorities, 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 respects the privacy of materials of certificate subscribers and ensures the compliance with the relevant national regulations and laws on privacy protection. Meanwhile, iTrusChina will ensure that all staff strictly comply with the internal working system and regulations.

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/CPS.

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 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/CPS and related operation management work documents. According to the Mozilla Root Policy, Mozilla can use this CP/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/CPS.

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/CPS.

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 subscriber information in the certificate is verified.

iTrusChina is not responsible for assessing whether the certificate is used within the appropriate range, and the subscriber and the relying parties 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/CPS;

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 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;

6) Verify the identity of the applicant in accordance with the requirements of Section 3.2 of this CP/CPS;

7) RA will submit service applications for revocation and renewal, etc. to iTrusChina in time according to the regulations of CP/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) The subscriber has read, known and accepted the responsibility clauses in the subscriber agreement of iTrusChina's and all the terms and conditions in this CP/CPS when applying for a certificate.

2) The subscriber should 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 certificate are true, complete and accurate. In case of any changes in the foregoing information, materials or statements, the subscriber shall notify RA in time in written form. 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 written form 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/CPS, 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 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 written form and terminate using the certificate immediately.

8) 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) The subscriber shall use certificate within the range specified in this CP/CPS 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 CP/CPS and the relying party agreement, agree to comply with all the provisions and constraints of this CP/CPS and the relying party agreement, and agree to the provisions of this CP/CPS 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/CPS 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 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/CPS.

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, that has been 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/CPS.

9.9 Indemnities

9.9.1 Indemnification by CAs

iTrusChina only bears the liability for the direct loss of the certificate subscriber and the relying party due to its own reasons, and bears no liability for the indirect loss.

The liability of indemnification that iTrusChina bears for direct loss is limited to: The compensation for each server certificate shall not exceed 10 times the purchase price of the certificate, and the compensation for each subscriber or each relying party for each EV server certificate shall not be less than 2 thousands US Dollars.

If iTrusChina violates the statement in Section 9.6.1 of this CP/CPS, the end entities, such as the certificate subscriber and the relying party, may apply for indemnity (except for statutory or agreed liability exemptions). In case of the following cases, iTrusChina bears limited liability of indemnification:

1）iTrusChina has issued the certificate to the third party other than the subscriber by mistake, causing the subscriber or the relying party to suffer losses;

2）Under the circumstance that the subscriber submits true, complete and accurate information or materials, the certificate issued by iTrusChina has wrong information, causing the subscriber or the relying party to suffer losses;

3）Under the circumstance that iTrusChina knows that the subscriber has submitted false information or materials and still issued a certificate to the subscriber, causing the relying party to suffer losses;

4）Due to iTrusChina's reasons, the private key of the certificate is deciphered, stolen and compromised, causing the subscriber or the relying party to suffer losses;

5）iTrusChina failed to revoke the certificate in time, causing the relying party to suffer losses.

In addition, the indemnity limit of iTrusChina is specified as follows:

1）All indemnification obligations of iTrusChina shall not exceed the upper limit of the indemnity , the upper limit of indemnity can be reformulated by iTrusChina according to the specific circumstance, and iTrusChina will immediately notify the parties concerned of the circumstance after the reformulation.

2）Regarding the losses caused by subscribers or relying parties, iTrusChina does not bear any liability of indemnification, which shall be undertaken by subscribers or relying parties on their own.

3) Regarding the loss incurred during the valid period of the certificate, the subscriber or the relying party shall lodge a claim in written with iTrusChina within three years from the date of knowing or should know the occurrence of the loss; the claim becomes invalid after the period of three years.

9.9.2 Indemnification by Subscribers

A subscriber shall bear the liability of indemnification if any of the following circumstances causes losses to iTrusChina and relying parties:

1）iTrusChina and its RAs or the third party with its authorization suffer damages due to the subscriber's intention, negligence or malice of providing untrue, incomplete and inaccurate information while applying certificate;

2）The certificate private key has been compromised intentionally or negligently, subscriber knows that the private key has been compromised and lost without timely notification of iTrusChina and its RAs, resulting in the damage for iTrusChina and its RAs and the third party;

3）The subscriber's usage of certificate violates this CP/CPS and related operation rules, or the subscriber applies the certificate to the business range not specified in this CP/CPS;

4）During the period from the certificate subscriber or other entities that have the right to applying revoke the certificate make a revoke request to iTrusChina publishes the revocation information of the certificate, if the certificate is used for an illegal transaction, or if a dispute occurs during the transaction, and if iTrusChina has performed the relevant operations in accordance with the specifications of this CP/CPS, the certificate subscriber shall bear all liabilities for compromise before the publication of the revocation information;

5）The information in the certificate has changed but the subscriber fails to stop using the certificate and fails to timely notify iTrusChina and its RAs;

6）No effective protection measures are taken for the private key, resulting in the loss or being damaged, stolen, compromised of the private key;

7）When knowing the private key is lost or at risk of being compromised, the subscriber fails to stop using the certificate and fails to timely notify iTrusChina and its RAs;

8）The subscriber uses the certificate beyond the valid period of the certificate;

9）The subscriber's certificate information infringes the intellectual property rights of a third party;

10）The subscriber uses the certificate beyond the prescribed range and purposes, such as engaging in criminal activities.

9.9.3 Indemnification by Relying Parties

In the following circumstances leads to the loss of iTrusChina the relying party bears the liability :

1）The relying party fails to enforce the obligations of iTrusChina and the relying party or the obligations stipulated in this CP/CPS, resulting in damage to iTrusChina and its RAs or third parties;

2）The relying party fails to make reasonable audits of certificates in accordance with the provisions of this CP/CPS, resulting in damage to iTrusChina and its RAs or third parties;

3）The relying party fails to verify the trust anchor of the certificate, resulting in damage to iTrusChina and its RAs or third parties;

4）The relying party fails to confirm whether the certificate is revoked by querying CRL or OCSP, resulting in damage to iTrusChina and its RAs or third parties;

5）The relying party trusts certificates in unreasonable circumstances, such as the circumstance that the relying party trust a certificate when it knows that the certificate is used beyond the prescribed range or period, or the certificate has been or may be compromised.

9.10 Term and Termination

9.10.1 Term

The CP/CPS comes into effect at 0:00 on the effective date. This CP/CPS becomes invalid on the day when the next version of CP/CPS becomes effective or when iTrusChina terminates the electronic certification service.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

After the termination of this CP/CPS, 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/CPS are still applicable, including, but not limited to, the contents of audit, confidential information, privacy protection, intellectual property, etc. in CP/CPS, as well as limited liability clauses relating to indemnification, and are still valid after this CP/CPS is terminated.

When some provisions in CP/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/CPS, 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/CPS compiling team reviews this CP/CPS at least once a year to ensure that it complies with national laws and regulations and meets the requirements of administration department, meets relevant international standards, and meets the actual needs of the certification business development.

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

9.12.2 Notification Mechanism and Period

The revised CP/CPS 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/CPS include: the inconsistency between the relevant contents of the CP/CPS 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 entities such as 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.

Regarding any lawsuit against iTrusChina or its RAs on any dispute involved in this CP/CPS, all parties concerned agree to submit it to the jurisdiction of People's Court in the local place of iTrusChina's industrial and commercial registration.

9.14 Governing Law

The CP/CPS 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/CPS 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/CPS.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The entire document structure of this CP/CPS 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/CPS, 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 this CP/CPS 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/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/CPS and a notice to the CA/B forum, as outlined above, must be made within 90 days.

9.16.4 Enforcement

In the case of disputes and lawsuits between iTrusChina, RA, the subscriber and the relying party, the winning party may ask the other party to pay the relevant legal costs as part of the indemnity. The exemption from a party's indemnity for one contract breach does not mean the exemption from indemnification for other contract breaches.

iTrusChina states that, if certificate subscriber, relying party or other entities fails to implement a provision in this CP/CPS, it is not considered that the entity will not implement this provision or other provisions in the future.

9.16.5 Force Majeure

When iTrusChina or its RAs do not have ability to provide normal services due to force majeure, such as natural disasters like earthquake, flood, lightning, and wars, etc., iTrusChina and its RAs do not bear losses caused to users.

9.17 Other Provisions

iTrusChina has the final interpretation right of this CP/CPS.

10. Annex

10.1 Annex A: iTrusChina's authentication for different types of certificates.

Type of Certificate	Authentication Requirements
DV SSL	1. iTrusChina will verify the applicant's control over the domain names or IP Address listed in a certificate as defined in this CP/CPS, Section 3.2.2.4 and Section 3.2.2.5. When using a random value, iTrusChina provides the unique random value for the certificate request, and the valid period of the random value will not exceed 30 days. 2. iTrusChina will check CAA records in accordance with the requirements of 3.2.2.8 of this CP/CPS. 3. iTrusChina will compare the information in the certificate request with the known high-risk application library maintained by iTrusChina itself. If any items match those in the high-risk application library but are not on the blacklist, Subscribers must provide a "Subscriber Authorization Letter" for additional verification. If the materials are qualified, the certificate issuance will proceed. If the materials do not meet the requirements or the information in the certificate request matches the blacklist, the certificate application will be rejected. iTrusChina reserves the right to reject certificate applications that pose legal and regulatory risks.
OV SSL	1. iTrusChina will verify the applicant's control over the domain names or IP Address listed in a certificate as defined in this CP/CPS, Section 3.2.2.4 and Section 3.2.2.5. When using a random value, iTrusChina provides the unique random value of the certificate request, and the valid period of the random value will not exceed 30 days. 2. iTrusChina will verify the applicant's organizational information in accordance with the requirements of 3.2.2.1 of this CP/CPS. 3. iTrusChina will verify the host country of the applicant in accordance with 3.2.2.3 of this CP/CPS.

	4. iTrusChina will confirm that the application has been effectively authorized in accordance with the requirements of 3.2.5 of this CP/CPS. 5. iTrusChina will check CAA records in accordance with the requirements of 3.2.2.8 of this CP/CPS. 6. iTrusChina will compare the information in the certificate request with the known high-risk application library maintained by iTrusChina itself. If any items match those in the high-risk application library but are not on the blacklist, Subscribers must provide a "Subscriber Authorization Letter" for additional verification. If the materials are qualified, the certificate issuance will proceed. If the materials do not meet the requirements or the information in the certificate request matches the blacklist, the certificate application will be rejected. iTrusChina reserves the right to reject certificate applications that pose legal and regulatory risks.
EV SSL	1. iTrusChina will verify the applicant's organizational information in accordance with the requirements of 3.2.2.1 of this CP/CPS. 2. iTrusChina will verify the host country of the applicant in accordance with 3.2.2.3 of this CP/CPS. 3. iTrusChina will verify the applicant's EV SSL subscriber identity as defined in this CP/CPS, Section 3.2.2.1.1. 4. iTrusChina will verify the applicant's control over the domain names listed in a certificate as defined in this CP/CPS, Section 3.2.2.4. When using a random value, iTrusChina provides the unique random value of the certificate request, and the valid period of the random value will not exceed 30 days. 5. iTrusChina will confirm that the Certificate Requester, Certificate Approver and Contract Signer has been effectively authorized in accordance with the requirements of 3.2.5 and 3.2.2.1.1 of this CPS. 6. iTrusChina will check CAA records in accordance with the requirements of 3.2.2.8 of this CP/CPS.

	7. iTrusChina will compare the information in the certificate request with the known high-risk application library maintained by iTrusChina itself. If any items match those in the high-risk application library but are not on the blacklist, Subscribers must provide a "Subscriber Authorization Letter" for additional verification. If the materials are qualified, the certificate issuance will proceed. If the materials do not meet the requirements or the information in the certificate request matches the blacklist, the certificate application will be rejected. iTrusChina reserves the right to reject certificate applications that pose legal and regulatory risks.
Enterprise Document Signing certificate	1. iTrusChina will verify the applicant's organization information in accordance with the requirements in this CP/CPS 3.2.2.1. 2. iTrusChina will verify representative of the applicant's personal identity information in accordance with the requirements of this CP/CPS 3.2.3. 3. iTrusChina will verify the applicant's country in accordance with this CP/CPS 3.2.2.3. 4.iTrusChina will confirm that the application has been effectively authorized in accordance with the requirements of 3.2.5 of this CP/CPS. 5. iTrusChina will compare the information in the certificate request with the known high-risk application library maintained by iTrusChina itself. If any items match those in the high-risk application library but are not on the blacklist, Subscribers must provide a "Subscriber Authorization Letter" for additional verification. If the materials are qualified, the certificate issuance will proceed. If the materials do not meet the requirements or the information in the certificate request matches the blacklist, the certificate application will be rejected. iTrusChina reserves the right to reject certificate applications that pose legal and regulatory risks.

Individual Document Signing certificate	1. iTrusChina will verify the applicant's personal identity information in accordance with the requirements of this CP/CPS 3.2.3. 2. iTrusChina will verify the entrusted person's personal identity information in accordance with the requirements of this CP/CPS 3.2.3.and confirm that the application has been effectively authorized in accordance with the requirements in this CP/CPS 3.2.5 if regarding an application that is made by an entrusted person. 3. iTrusChina will verify the applicant's country in accordance with this CP/CPS 3.2.2.3. 4. iTrusChina will compare the information in the certificate request with the known high-risk application library maintained by iTrusChina itself. If any items match those in the high-risk application library but are not on the blacklist, Subscribers must provide a "Subscriber Authorization Letter" for additional verification. If the materials are qualified, the certificate issuance will proceed. If the materials do not meet the requirements or the information in the certificate request matches the blacklist, the certificate application will be rejected. iTrusChina reserves the right to reject certificate applications that pose legal and regulatory risks.
Time Stamping Certificate	1. iTrusChina will verify the applicant's organizational information in accordance with the requirements of 3.2.2.1 of this CP/CPS. 2. iTrusChina will verify the host country of the applicant in accordance with 3.2.2.3 of this CP/CPS. 3. iTrusChina will confirm that the Certificate Requester has been effectively authorized in accordance with the requirements of 3.2.5 of this CP/CPS. 4. iTrusChina will compare the information in the certificate request with the known high-risk application library maintained by iTrusChina itself. If any items match those in the high-risk application library but are not on the blacklist, Subscribers must provide a "Subscriber

	Authorization Letter" for additional verification. If the materials are qualified, the certificate issuance will proceed. If the materials do not meet the requirements or the information in the certificate request matches the blacklist, the certificate application will be rejected. iTrusChina reserves the right to reject certificate applications that pose legal and regulatory risks.

10.2 Annex B: CA certificate information

Root certificate information

Root name	vTrus Root CA	vTrus ECC Root CA
Country	CN	CN
Organization	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
Common name	vTrus Root CA	vTrus ECC Root CA
Serial No.	43e37113d8b359145db7ce8cfd35fd6fbc058d45	6e6abc59aa53be983967a2d26ba43be66d1cd6da
Start date	2018-07-31 15:24:05	2018-07-31 15:26:44
End date	2043-07-31 15:24:05	2043-07-31 15:26:44
Algorithm	RSA(4096 bits)	ECC(384 bits)
SHA 256Fingerprint	8A:71:DE:65:59:33:6F:42:6C:26:E5:38:80:D0:0D:88:A1:8D:A4:C6:A9:1F:0D:CB:61:94:E2:06:C5:C9:63:87	30:FB:BA:2C:32:23:8E:2A:98:54:7A:F9:79:31:E5:50:42:8B:9B:3F:1C:8E:EB:66:33:DC:FA:86:C5:B2:7D:D3
Signature algorithm	sha256RSA	sha384ECDSA

Sub CA information

Certificate name	vTrus DV SSL CA	vTrus ECC DV SSL CA

Country	CN	CN
Organization	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
Common name	vTrus DV SSL CA	vTrus ECC DV SSL CA
Issuer	vTrus Root CA	vTrus ECC Root CA
Serial No.	47b6120febd5e7254c99de1cdcdd535ad35f9976	1466a82cbf0183aa093fd2280fac3c0e39f02940
Start date	2023-12-13 11:21:40	2023-12-13 11:25:48
End date	2033-12-10 11:21:40	2033-12-10 11:25:48
Algorithm	RSA(2048 bits)	ECC(256 bits)
SHA256Fingerprint	0A85075DD6B382EAB31449823DB8BED6B61A441714165E33FACA42CD9C8DEC2A	4D391FC790BD702CAD3CCBC0B025C5CDD88C6FDF274DCF5FBD3F027A80C2C7E5
Signature algorithm	sha256RSA	sha384ECDSA

Certificate name	vTrus YunSSL DV CA	vTrus FastSSL CA G1
Country	CN	CN
Organization	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.

Common name	vTrus YunSSL DV CA	vTrus FastSSL CA G1
Issuer	vTrus Root CA	vTrus Root CA
Serial No.	1ff2f88b5bf9fd738bec90abafdb501afe74eada	4815cbde3d2be06475f3793fb94e64a073d21bfa
Start date	2023-12-13 11:16:17	2023-12-13 11:18:07
End date	2033-12-10 11:16:17	2033-12-10 11:18:07
Algorithm	RSA(2048 bits)	RSA(2048 bits)
SHA 256Fingerprint	A7D7285843B89B134F852CB52A6F431938257C826D699AA806C894A0A1CDB847	3B83EB5D7A9A5AF06275A0A1C1B35BD562622A5521E2699F25559328B8829058
Signature algorithm	sha256RSA	sha256RSA

Certificate name	vTrus OV SSL CA	vTrus ECC OV SSL CA
Country	CN	CN
Organization	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
Common name	vTrus OV SSL CA	vTrus ECC OV SSL CA
Issuer	vTrus Root CA	vTrus ECC Root CA
Serial No.	230301e5d69ac8930d623394ffd2a0917c0e7e7b	460a8546796fd139ba62ed86d76346942129b7a4
Start	2023-12-13 11:19:22	2023-12-13 11:23:58

date		
End date	2033-12-10 11:19:22	2033-12-10 11:23:58
Algorithm	RSA(2048 bits)	ECC(256 bits)
SHA 256Fingerprint	2CF5539249A9E38FC010E29FF3E8046658F3D030B93310473687FA91F8DA44CA	42E46C4487459128517649731457B6AE20099D541BD182C5497B2E67E6FFD0F6
Signature algorithm	sha256RSA	sha384ECDSA

Certificate name	vTrus EV SSL CA	vTrus ECC EV SSL CA
Country	CN	CN
Organization	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
Common name	vTrus EV SSL CA	vTrus ECC EV SSL CA
Issuer	vTrus Root CA	vTrus ECC Root CA
Serial No.	7d746ea36e2136270e8fc2e2456d229cb90c80b7	302282d66df3b37a7f5bf373d4ae8e7c5c125376
Start date	2018-07-31 15:31:06	2018-07-31 15:39:20
End date	2038-07-31 15:31:06	2038-07-31 15:39:20
Algorithm	RSA(2048 bits)	ECC(256 bits)
SHA 256Fingerprint	F3:AA:6D:71:2A:15:F6:3F:83:50:80:49:79:DB:54:24:19:A6:1B:2B:1D:22:E7:56:C4:17:AB:FE:8D:74:A3:CA	BD:30:C0:D1:E7:AC:B8:3E:FC:4F:5F:6C:62:F8:F3:A5:79:BA:B2:75:27:AF:AE:66:6C:69:6C:3A:86:71:75:F1
Signature	sha256RSA	Sha256ECDSA

algorithm		

Certificate name	vTrus Document Signing CA	vTrus Time Stamping CA
Country	CN	CN
Organization	iTrusChina Co.,Ltd.	iTrusChina Co.,Ltd.
Common name	vTrus Document Signing CA	vTrus Time Stamping CA
Issuer	vTrus Root CA	vTrus Root CA
Serial No.	4ecf532a91cd6844cdc6839b66110ab2d2d9319b	13ac9f0f9b2fe210e06a96888c4eee1c49040ea4
Start date	2021-10-14 11:24:59	2021-10-14 11:28:32
End date	2041-10-14 11:24:59	2041-10-14 11:28:32
Algorithm	RSA(2048 bits)	RSA(4096 bits)
SHA 256Fingerprint	B5C3EFC7BA547B66318C23C93E0FB18301DB84ADA233B19C9F2F26F5D64C3559	F7291D1E8BCC7583AC3FA83977C6C5EBC784A118A397647A9FC37EF85E14DF5C
Signature algorithm	sha256RSA	sha256RSA

Certificate name	ITC-Digicert SignBridge
Country	CN
Organization	iTrusChina Co.,Ltd.
Common name	ITC-Digicert SignBridge
Issuer	vTrus Root CA
Serial No.	558037c556be6bac389a1752c47f04c0013aa761
Start date	2024-06-19 15:25:50
End date	2039-06-19 15:25:50
Algorithm	RSA(2048 bits)

SHA 256Fingerprint	E4DE27EC980401A68E29F257248AF1ACCBEFEF94C6DCDF5C0848394ADC9FD203
Signature algorithm	sha256RSA