Certification Practice Statement
Of
CFCA Global-Trust System

V2.1

November 2014

History of Changes

Version	Action	Description	Modified By	Reviewed/ Approved By	Effective Date
1.0	**Draft, review and approve the first version.**			**Security Committee**	**October 2011**
2.0	**Add**	**Add description and requirements on EV systems and OCA21; add description of certificate types and keys.Form the draft of Version 2.0.**	**ZHAO Gaixia**		
	Amend	**Amend related content according to the review of the Security Committee on April 7, 2013.**	**ZHAO Gaixia**	**Security Committee**	**April 2013**
2.0.1	**Amend**	**Amend / Add related content in order to comply with lateset Baseline Requirement**	**ZHAO Gaixia**	**Security Committee**	**March 2014**
2.1	**Amend**	**Amend related content in order to resolve issue raised in Mozilla Public discussion in June 2014**	**ZHAO Gaixia**	**Security Committee**	**Nov 2014**

Table of Contents

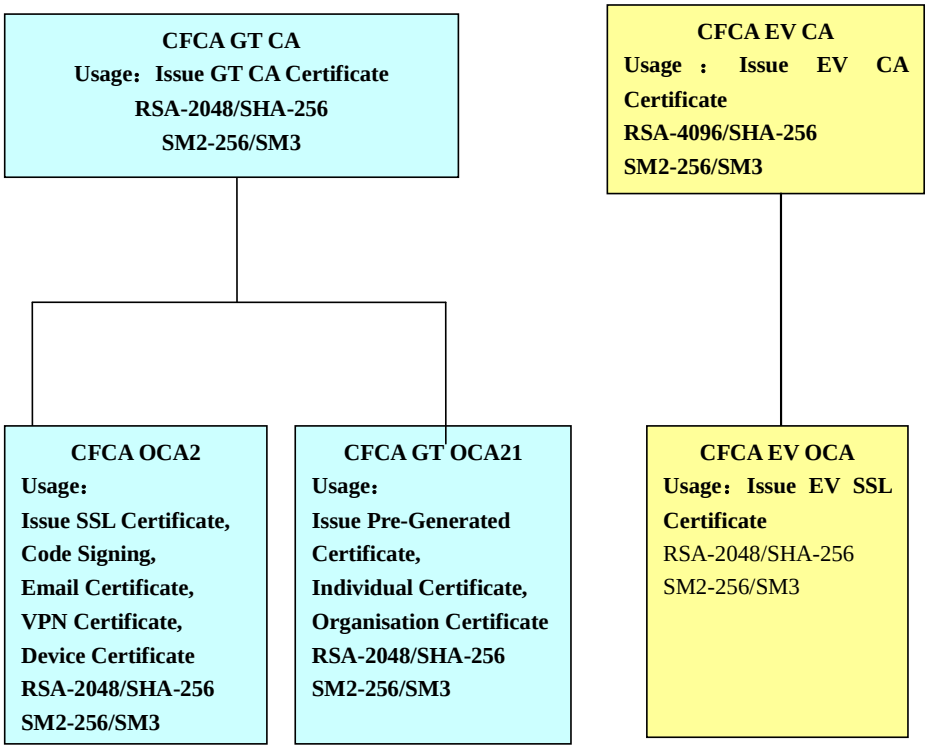
1 Introduction

1.1 Overview

Established on June 29, 2000, China Financial Certification Authority (CFCA) is a national authority of security authentication approved by the People's Bank of China and state information security administration. It's a critical national infrastructure of financial information security and is one of the first certification service suppliers granted a certification service license after the release of the Electronic Signature Law of the People's Republic of China.A Certification Practice Statement (CPS) is a detailed description and statement of the practices which a certification authority (CA) employs in the whole life cycle of digital certificates (certificates for short) (e.g. issuance, revocation, andrenew). It also describes the details of the business, technologies and legal responsibilities.

This CPS presents practices under the CFCA Global Trust System. The System constitutes of CFCA GT CA system and CFCA EV CA system. The former includes CFCA GT OCA2 and CFCA GT OCA21, while the latter includes CFCA EV CA and CFCA EV OCA. The following figure shows the system structure.

CFCA Global Trust System



All the subordinate CAs of CFCA are owned and controlled by the CFCA directly.

This CPS conforms to: IETF RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework); the《Electronic Signature Law of the People's Republic of China》 approved by the Tenth NPC and enforced on April 1, 2005; the《Specification of Cryptography and Related Security Technology for Certificate Authentication System》, and

《Administration of Electronic Certification Services》 realeased by the State Cryptography Administration; the 《Methods for the Administration of Electronic Certification Services》, 《Specification of Electronic Certification Practices (Trial Version)》 enacted by the Ministry of Industry and Information Technology of the People's Republic of China; Web Trust 2.0, Guidelines for the Issuance and Management of Extended Validation Certificates 1.4, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificatess 1.1.6, and other common practice norms of CA.

CFCA meets the requirements of WebTrust and has been audited by external auditors. CFCA holds a valid License of Electronic Certification Services issued by MIIT, the competent department of CFCA.

1.2 Document Name and Indentification

This document is the Certification Practice Statement of CFCA Global-Trust System (CFCA Global-Trust CPS).

CFCA has registered the corresponding Object Identity (OID) of this document in the National Registraion Center for OID. The OID of this document is 2.16.156.112554. Those of the GT CA and EV CA are 2.16.156.112554.2.1 and 2.16.156.112554.3 respectively.

1.3 Electronic CertificationParticipants

Electronic certificationparticipants appear in this document include: Certification Authorities, Registration Authorities, Relying Parties and other participants. Following is the description.

1.3.1 Certification Authorities

A Certification Authority (CA) is responsible for certificate issuance, renew and revocation, key management, certificate status information service, release of Certificate Revocation List (CRL) and policy formulation, etc.

1.3.2 Registration Authorities

A Registraion Authority (RA) is responsible for the acceptance, approval and management of subscriber certificates. It deals with the subscribers and deliveries certificate management information between the subscribers and the CA.

The RA function of the OCA2 and EV OCA system under the CFCA Global Trust System is performed by CFCA internally. The RA function of the OCA21 can be delegated to other organizations according to relevant norms.

1.3.3 Subscribers

Subscribers are the entities of certificates issued by CFCA.

It should be noted that, "Subscriber" and “Subject" are two different

termsused in this CPS to distinguish between two different roles: "Subscriber", is the entity，individual and organization generally， which contracts with CFCA for the issuance of certificates and; “Subject", is the entity which the certificate is bound to. The “subject” of sever certificates refer to trusted sever or a device used to keep secure communication with other parties. The Subscriber bears ultimate responsibility for the use of the certificate but the Subject is the individual that is authenticated when the certificate is presented.

1.3.4 Relying Parties

A relying party is an individual or organization that acts on reliance of the trust relations proved by the certificates.

1.3.5 Other Participants

Others beside CFCA, subscribers and relying parties are refered to as Other Participants.

1.3.6 Beneficiaries and Responsibilities

Participants related to the CFCA Global Trust System are all beneficiaries. The benefits are listed below.

1. Beneficiaries

Beneficiaries of certificates may be:

(1) The subscriber entering into the Subscriber Agreement for the certificate;

(2) The applicant who obtained the certificate;

(3) All application software vendors who have obtained certificates;

(4) All relying parties that actually rely on such certificates during their validity periods.

2. Certificates provide the following warranties:

（1） Legal Existence: CFCA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the Certificate was issued, the Subject named in the Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;

（2） Right to Use Domain Name or IP Address: CFCA verifies that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension. (Detail in Section 3.2)

（3） Authorization for Certificate: CFCA verifies that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject. (Detail in Section 3.2)

（4） Accuracy of Information: CFCA verifies the accuracy of all of the information contained in the Certificate. (Detail in Section 3)

（5） Identity of Applicant: if the Certificate contains Subject Identity Information, CFCA verifies the identity of the Applicant in accordance with

Sections 3.2.2;

（6） Subscriber Agreement: Subscriber and CFCA will be parties to a legally valid and enforceable Subscriber Agreement that satisfies related Requirements.

（7） CFCA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates.

（8） Revocation: CFCA will promptly revoke the Certificate upon the occurrence of any revocation event according to CPS.

1.4 Certificate Usage

1.4.1 CFCA Certificate Types and Appropriate Uses

	Indivdual Normal	Individual Advanced	Enterprise Normal	Enterprise Advanced	server	VPN	Code-Signing	Secure Email	Device
OCA2					√（SSL）	√	√	√	√
OCA21	√	√	√	√					
EVOCA					√（EV SSL）				

CFCA GT CA and CFCA EV Root are only used for signing subordinate CA certificates

1.4.1.1 CFCA SSL Global Server Certificate

CFCA SSL Certificate includes Wildcard Certificate and Multi-Domain Certificate. SSL Certificates can be used in the areas such as online banking, e-commence, e-politic, enterprise informatization and public services and so on.

They create a safe tunnel between the browser and the web server for encrypted transmission of data, and prevent information leakage. The subscribers and relying Parties can verify the authenticity and reliability of the website through Server Certificate authentication. SSL Certificates provide fundamental trust service for building trustworthy networks. CFCA SSL Certificates are issued by CFCA GT OCA2. Their key sizes are RSA-2048 or SM2-256.

1.4.1.2 CFCA EV SSL Certificate

CFCA EV SSL Certificates are Server Certificates issued after stringent identity verification to ensure secure information transmission between the website and the clients and provides more detailed authentication information.

The purposes of the EV SSL Certificates issued by CFCA are as follow:

1. Primary Purposes

The primary purposes of EV Certificates are to:

（1）Identify the authenticity and reliability of the website users visit: if the website users accessing to uses the EV SSL certificate issued by CFCA, which means that this website is controlled by a legal entity and its name, address and registration information have been verificated. Plus, any content in this website is real and reliable.

（2）Enable encrypted communications transferred between the client-side and sever: Exchanging encryption keys can enable the

encrypted communication information over the Internet between the user of an Internet browser and a website.

2. Secondary Purposes

EV Certificates may help to:

（1） It is more difficult to apply the EV certificate than the ssl certificate, as EV certificate application needs relatively more detailed information. Using the EV certificates could effectively prevent phishing websites and other online identity fraud attacks;

（2） Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves and their legitimate websites to users;

（3） Assist law enforcement in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

3. Excluded Purposes

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV Certificate is not intended to provide any assurances, or otherwise represent or warrant:

(1)That the Subject named in the EV SSL Certificate is actively engaged in doing business;

(2)That the Subject named in the EV SSL Certificate complies with

applicable laws;

(3)That the Subject named in the EV SSL Certificate is trustworthy, honest, or reputable in its business dealings;

(4)That it is “safe” to do business with the Subject named in the EV SSL Certificate.

The EV SSL Certificate is issued by CFCA EV OCA.

1.4.1.3 CFCA Pre-Generated Certificate

Pre-Generated Certificate is an extended business of CFCA. The process of Pre-Generation Certificate issuance is described below. CFCA signs a cooperative agreement with the RA. According to the demands of its business, RA entrusts CFCA to generate certificates for its users in a secure environment. Then RA authenticates the Subscribers’ identities. It then binds the Pre-Generated Certificates with the Subscribers’ information. The Certificates can then be used in registrants’ applications. CFCA Pre-Generated Certificate is issued by CFCA GT OCA21.

1.4.1.4 Individual Certificate

Individual Certificate, including Personal Certificate and Corporate Employee Certificate, is used to distinguish, indentify and verify the indentity of the individual. There are two types: Ordinary Individual Certificate and Advanced

Individual Certificate. The former is used in ID verification and signing. The latter is used for ID verification, encryption and signing to ensure confidentiality, completeness and non-repudiation of the information. CFCA Individual Certificate is issued by CFCA GT OCA21.

1.4.1.5 Corporate Certificate

Corporate Certificate is used to distinguish, identify and verify the identity of the enterprise. There are two types: Ordinary Corporate certificate and Advanced Corporate certificate. The former is used for enterprise ID verification and signing. The latter is used for ID verification, data encryption and decryption, signing on orders and contracts to ensure the confidentiality, completeness and non-repudiation of information. CFCA Corporate certificate is issued by CFCA GT OCA21.

1.4.1.6 Device Certificate

Device Certificate is used to identify the server or operation device, etc. It encrypts or decrpyts the interactive data of the device, and ensures the completeness and security of data transmission. CFCA Device Certificate is issued by CFCA OCA2.

1.4.1.7 VPN Certificate

VPN Certificate is used to identify VPN gateway, authenticate the client and

the VPN gateway, and ensures secure transmission of interactive data. CFCA VPN Certificate is issued by CFCA OCA2.

1.4.1.8 Email Certificate

Email Certificate binds the email address with the Subject named in the Certificate to authenticate the identity of the owner of the email address. It's also used to encrypt and decrypt the information transmitted through email, and to sign the email. CFCA email certificate is issued by OCA 2.

1.4.1.9 Code Signing Certificate

Code Signing Certificate is used to identify the owner of the code, to sign when code is released, in order to ensure the completeness and security of the code. CFCA code signing certificate is issued by OCA 2.

1.4.2 Restricted Certificate Uses

The certificates' functions are restricted according to their types. For example, CFCA EV SSL Certificate can only be used on web servers that have undergone stringent authentication.

The intended key usages are described in the extensions of the subscriber certificates. However the effectiveness of the restriction depends on the

applications. Therefore, if the participants fail to follow such restriction, their interests are not protected by CFCA.

1.4.3 Prohibited Certificate Uses

Certificates under the CFCA Global Trust System cannot be used in applications that violate any national or local law and regulation.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization administering this document is the Business Management Department of CFCA. It sets up the “CPS Team” to compile or amend this CPS when needed. The General Manager can also set up a temporary CPS Team and appoint a person to take charge of the drafting or revision.

1.5.2 Contact

Any question on this CPS, please contact the Business Management Depatment:

Phone: 010-83526220

Fax: 010-63555032

Email: cps@cfca.com.cn

Address: NO.20-3, Pingyuanli, Caishikou Nandajie Street, Xicheng District, Beijing, China

1.5.3 Department Dertermining CPS Suitability for the Policy

The CPS team is responsible for compiling the draft or revision of the CPS, and submitting it to the Security Committee to review. The Security Committee reviews the CPS and determinies whether it is in conformity with relevant requirements. If yes, the CPS will be submitted to the approval of the General Manager. Once approved, the CPS will be publicized, and will be reported to the competent department within 20 days following the publication.

1.5.4 CPS Approval Procedures

The CPS Team compiles a draft for discussion, which will be amended according to the opinions of the leaders and managers, resulting in a draft for review.

The CPS Team submits the draft for review to the Security Committee, and amends the draft afterwards according to the opinions of the Committee. The draft then goes to the Business Management Department, who determines the format and version number of the CPS. At this point, a final version is ready.

After being reviewed by the leaders and managers, the final version is submitted to the General Manager for approval. Once approved, it can be publicized in a form that aligns with the requirements of relevant authorities. The CPS is posted on CFCA website (http://www.cfca.com.cn). Paper CPSs are

delivered to the clients and partners. The Business Management Department coordinates related parties in the publication.

The online publication of the CPS follows the 《CFCA Website Management Methods》. CPSs publicized in other forms should be consistent with the one posted on the website. The Business Management Department will report the CPS to the competent department within 20 days following the publication.

Periodic (usually annual) reviews are performed by the Business Management Department to determine if revision if needed. The other departments can also raise a revision request depending on the demands of business. The CPS can also be modified according to the relevant standards that the CPS complies to.

If pervasive revision is needed, CFCA will adopt the same procedures of making the first version. If minor revision is needed, the Business Management Deparment will revise the CPS and submit it to the leaders and managers to review. The CPS, once approved by the General Manager, will be released on the corporate website. Every revised CPS will be reported by the Business Management Department within 20 days following the publication.

1.6 Definitions and Acronyms

Please refer to Appendix Definitions and Acronyms.

2 Publication and Repository Responsibilities

2.1 Repositories

CFCA provides information services to the subscribers and relying parties through its repositories, which contains: Certificates, CRL, CPS, CP, Certificate Service Agreement, technical support manual, CFCA website information and adhoc information released by CFCA.

2.2 Publication of Certification Information

CFCA releases CPS, CP and techinal support information on its website. Subscriber certificates can be obtained on the CFCA Certificate download platform. The certificates issued by OCA2 and EV OCA can only are obtained through the repositories. Information of revoked Certificates is available on the CRL website, while the certificate status information (valid, revoked or suspended) is available through OCSP services.

2.3 Time or Frequency of Publication

CPS, CP and relevant documents will be released on the CFCA website within 15 days after they have gone through the procedures stated in Section 1.5.4. They are accessible 7*24 hours. CRL information issued by OCA2 and EV OCA will be updated within 24 hours; while that by OCA21 within three hours. The frequency of CRL publication can be tailored according to the demands of the subscribers.

Manual real-time publication of CRL is also applicable if needed.

2.4 High Risk Reporsitory

CFCA maintains theinternal database that includes previously revoked certificates (including EV Certificates) and previously rejected certificate requests, due to suspected phishing or other fraudulent usage. This information is used to flag new Certificate Requests of the corresponding applicants as of significant risks.

Prior to identity verification, CFCA refers to the lists of entities with high risks. If the applicant is one of the entities most vulnerable of phishing and fraudulent identity attacks, it's flagged as an "applicant of high risk" during the applying stage.

Entities with high risks include:

1) Those on the phishing target lists of APWG and APAC;

2) Applicants of previously revoked SSL Certificates, EV SSL Certificates, and previously rejected Certificate Requests, due to suspected phishing or other fraudulent usage. CFCA would mark these applicants as High Risk Applicants as the basis for identification of high risk instituions.

The CFCA does not process the applications from high risk applicants.

2.5 Access Controls on Repositories

Edit and wirte access is restricted to only authorized personnel. Read only access is unrestricted.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of Names

Depending on the Certificate types, Subject name can be that of an individual, organization, sector, domain and device, and also can be the combination of organization and individual information. The naming follows the X.500 Distinguished Name Standard. Please refer to Section 7.1.4 for details.

3.1.2 Need for Names to be Meaningful

DN (Distinguished Name): A unique X.500 name put in the field of Subject Name on the Certificates to identify the subject. Except for Pre-Generated Certificates, the content put in this field must reflect the authentic identity of the subject, be meaningful and in line with laws.

For Individual Certificate, the Common Name (CN) in the DN usually contains the person’s real name or ID number, and is verified as the key information.

For Corporate certificate, the CN usually contains organization name or ID number, and is verified as the key information.

For Pre-Generated Certificate, the DN contains the identifier of the RA system used to verify the indentity of the subscriber. The identifier in the RA system and the subscriber information are identified and verified together.

For the EV SSL Certificate, the CN can only be the domain name owned by the subscriber. It's identified and verified with the other information of the subscriber.

For SSL Certificate, the CN can be the domain name or external IP owned by the subscriber. It's identified and verified with the other information of the subscriber.

For VPN Certificate and Device Certificate, the CN can be the name or IP address of the device owned by the subscriber. It's identified and verified with the other information of the subscriber. Effective from May 1, 2014, CFCA does not accept certificate application for reserved IP address or internal domain name. The previously issued certificates with reserved IP address ore reserved domain name would be revoked and replaced by Oct 1, 2016.

For Email Certificate, the CN must be the real name; the email address must be valid.

For Code-signing certificates, the DN must be the subscriber's real name, and the CN can be the code name or name on the valid ID. CFCA would verify the ID provided.

3.1.3 Anonymity or Pseudonymity of Subscribers

Certificate Requests submitted in anonymity fail to meet the requirement of CFCA, and will not pass the verification. No certificate or service will be provided in this case.

Certificates using pseudonymity are invalid, and will be revoked once the situation is confirmed.

3.1.4 Rules for Interpreting Various Name Forms

Please refer to Section 7.1.4 for the DN naming rules of CFCA.

3.1.5 Uniqueness of Names

CFCA ensures that the Subject Distinguished Name of the subscriber is unique within the trust domain of CFCA.

3.1.6 Recognition, Authentication, and Role of Trademarks

The subscribers shall warrant to CFCA and provide a statement to relying parties that: the information submitted in certificate application has not, in any form, infringed the Intellectural Property Rights of other, including the ownership of trade name, corporate name and etc. The Certificates issued by CFCA does not contain any trademarks or other information which may infringe other parties' rights.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The method to prove possession of a private key by the subscriber is the digitial signature in pkcs#10. Before CFCA issues a certificate, the system automatically uses the public key of the subscriber to validate the effectiveness of the signature of the private key, as well as the completeness of application information, and thus determines whether the subscriber owns the private key.

3.2.2 Authentication of Subscriber Identity

Prior to applying for a certificate under the Global Trust System, the subscriber should appoint a requester and issue a written letter of authorization. The requester should provide valid ID proof, certifcate application materials, acknowledge relevant stipulation and agree to bear corresponding responsibilities. Subscribers must submit the certificate request form and the terms of agreement, but other application materials may vary for different types of certificates requested and different types of subscribers.

A subscriber should agree with the terms of agreement before the application could be processed. The terms of agreement contains:

1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CFCA, both in the certificate request and as otherwise requested by the CFCA in connection with the issuance of the

Certificate(s) to be supplied by the CFCA;

2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;

5. Reporting and Revocation: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CFCA to revoke the Certificate, in the event that: (a) anyinformation in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;

6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. Responsiveness: An obligation to respond to the CFCA's instructions

concerning Key Compromise or Certificate misuse within a specified time period.

8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CFCA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CFCA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

Upon receiving the application, CFCA or the RA authorized by CFCA will authenticate subscriber identity, and store the application materials according to the agreement. The longest interval of identity verification for the subscribers of SSL Certificates is 39 months.

Identity verification procedures are as follow:

The account managers of the Marketing Department and Sales Department collect application materials. The Business Management Department verifies the materials and the subscribers' identities. RA system operators input the application information. RA system reviewers review the inputed information and assist the subscribers to download the Certificates.

3.2.2.1 Authentication of Individual Identity

When individuals apply for the Certificates, they should provide CFCA or the RA authorized by CFCA authentic and effective proofs of their identities. For individual applicants in organizations, the application materials should bear corporate seals or contain letters of authorization. CFCA will verify these

organizations.

The following materials should be submitted:

1. Certificate applicationForm;

2. Copies of ID;

3. Authorization of the organization (applicable only to the individuals in organizations).

The investigators verify the completeness and authenticity of the materials. Reliable data source would be used to validate the applicant's identity, address, country and etc.

3.2.2.2 Authentication of Corporate (Organization) Identity

Prior to applying for a certificate, oganization subscribers should authorize a staff to propose the certificate request, and provide authentic and effective proof of organization identity.

Following materials should be submitted:

1. Certificate applicationForm;

2. At least one type of organization ID;

3. The personal ID of the requester;

4. The authorization of the requester.

These materials should bear corporate seals.

The verification procedures of the organization subscriber are as follow:

First, CFCA designates a staff to receive the application materials, and carry out initial examiniation of the completeness. This is to ensure that the materials meet the demands for identity verification.

Second, CFCA designates an investigator to verify the application materials:

(1) Verify the organization identity, address, country and other information through third party channels or the identity repository of CFCA to ensure that the organization is an authentic existence.

(2) Verify the authorization through phone calls or official letters.

3.2.2.3 Authentication of SSL Certificate Subscriber Identity

Applications for SSL Certificates can only be submitted to CFCA, who accepts applications from both organizations and individuals. SSL certificates include certificates of multiple domain names and wildcard domain names. The following materials should be submitted:

1. Certificate applicationForm;

2. At least one type of organization ID (not applicable for individual subscribers);

3. ID of the applicants;

4. Authorization for the requester from the organisation (not applicable for individual subscribers);

5. Proofs of possession of public IP (not needed for domain validated certificates);

6. CSR file for the application.

CFCA verifies not only the ID, address, and country of the applicant, but also the IP and the compliance of CSR. The procedures are as follows:

CFCA performs a WHOIS inquiry on the internet for the domain name supplied by the applicant, to verify that the applicant is the entity to whom the domain name is registered. Where the WHOIS record indicates otherwise, CFCA will ask for a letter of authorization, or email to the register to inquiry whether the applicant has been authorized to use the domain name.

To verify the public IP, the subscriber can supply a sealed paper document or email from the ISP showing the IP is allocated by the ISP to the applicant.

For application for wildcard domain name certificates, CFCA will verify the corresponding sub FQDN. For certificates with multiple domain names, CFCA will verify all the domain names listed.

The CSR is verified to determine whether the CSR and the Certificate applicationForm are consistent; whether it’s in line with relevant norms, such as the order of DN; whether the applicant possesses the private key or not.

3.2.2.4 Authentication of EV SSL Certificate Subscriber Identity

Applications for EV SSL Certificates can only be submitted to CFCA. The subject must be the domain name of the web server, not the IP address. The domain name must not contain wildcards. EV SSL certificates could contain multiple domain names. The applicants can only be private organizations, business entities,

government entities and non-commercial entities and should meet the following requirements:

1. Business Entities

CFCA may issue EV Certificates to Business Entities including public companies、individual firms and state-owned enterprises that satisfy the following requirements:

(1) The organization MUST be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency, or Governing Body in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation) or is an entity that is chartered by a state regulatory agency;

(2) The organization MUST have designated with the Incorporating or Registration Agency, or Governing Body either a Registered Agent, or a Registered Office (as required under the laws of the Jurisdiction of Incorporation Registration) or an equivalent facility;

(3) The organization MUST not be designated on the records of the Incorporating or Registration Agency, or Governing Body by labels such as “inactive”、“invalid”、“not current” or the equivalent;

(4) At least one Principal Individual associated with the Business Entity MUST be identified and validated;

(5) The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;

(6) The organization MUST have a fixed place of business.

(7) The organization's Jurisdiction of Incorporation, Registration, Charter, or License and/or its Place of Business MUST NOT be in any country where CFCA is prohibited from doing business or issuing a certificate by the laws of CFCA's jurisdiction;

(8) The organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of CFCA's jurisdiction.

2. Non-Commercial Entity Subjects

CFCA may issue EV Certificates to Non-Commercial Entity including hospitals、schools that satisfy the following requirements:

(1) The legal existence of the Government Entity is established by the political subdivision in which such Government Entity operates;

(2) The organization MUST have a fixed place of business.

(3) The common name used by the organization MUST be on the behalf of it.

(4) At least one Principal Individual associated with the Business Entity MUST be identified and validated;

(5) The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;

(6) The Government Entity MUST NOT be in any country where CFCA is prohibited from doing business or issuing a certificate by the laws of CFCA's jurisdiction;

(7) The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of CFCA jurisdiction.

3. Organizations Subject

CFCA MAY issue EV Certificates to Organizations including social organizations、private non-enterprise units and foundations that satisfy the following requirements:

(1) The Organizations MUST be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction ,the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;

(2) The Organizations MUST have a verifiable physical existence and business presence;

(3) Where the organization represents itself under an assumed name, CFCA verifies the organization use of the assumed name.

(4) The Organization MUST NOT be in any country where CFCA is prohibited from doing business or issuing a certificate by the laws of CFCA's jurisdiction; and

(5) The Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of CFCA jurisdiction.

4. Government Entity Subjects

CFCA MAY issue EV Certificates to Government Entity including public security bureau、tax bureau whoqualify the following requirements:

(1) The Government Entity MUST be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction ,the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;

(2) The Government Entity MUST NOT be in any country where CFCA is prohibited from doing business or issuing a certificate by the laws of CFCA's jurisdiction; and

(3) The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of CFCA jurisdiction.

(1) International Organization Entity Subjects

(i) The International Organization Entity is created under a Charter, Treaty, Convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CAB Forum may publish a listing of International Organizations that have been approved for EV eligibility, and

(ii) The International Organization Entity MUST NOT be headquartered in any country where CFCA is prohibited from doing business or issuing a certificate by the laws of the CFCA's jurisdiction; and

(iii) The International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CFCA jurisdiction. Subsidiary organizations or agencies of qualified international organizations may also qualify for EV certificates issued in accordance with these Guidelines.

5. Role Requirements

The following Applicant roles are required for the issuance of an EV Certificate (letter of authorization is needed).

Certificate Requester: The EV Certificate Request MUST be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

Certificate Approver: The EV Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

Contract Signer: A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is

a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

The Applicant MAY authorize one individual to occupy two or more of these roles. The Applicant MAY authorize more than one individual to occupy any of these roles. EV certificate applicant MUST be a natural person who is an employee or the authorized agent (letter of authorization or proof materials is needed).

6. Domain Name of the Applicant

(1) The Applicant is the registered holder of the domain name or has been granted the exclusive right to use the domain name by the registered holder of the domain name

(2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization.

(3) The Applicant is aware of its registration or exclusive control of the domain name.

7、Documentation Requirements of EV Certificate Request

Subscribers can download the EV SSL Certificate Request form from the CFCA website. The Request contains related agreement, and subscriber warranties. By signing the Request, the subscribers sign the Subscriber Agreement of EV SSL Certificate. It’s legally binding.

When applying for CFCA EV SSL Certificates, the subscribers must submit

the following materials:

1) EV Certificate Request

The subscribers should provide the following information correctly according to the requirement of the request form:

Legal Organizaiton Name: The subscribers are not allowed to use common names.

Domain Name Information: The Applicant"s Domain Name(s) to be included in the EV Certificate;

Incorporating or Registration Agency: The name of the Applicant's Incorporating or Registration Agency;

ID Registration Number: The Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant"s Jurisdiction of Incorporation or Registration. If the Incorporating or Registration Agency does not issue Registration Numbers, then the date of Incorporation or Registration SHALL be collected;

Applicant Address: The address of the Applicant"s Place of Business, including –

(A) ☐Building number and street,

(B) ☐City or town,

(C) ☐State or province (if any),

(D) ☐Country,

(E) ☐Postal code, and

(F) ☐Main telephone number.

Certificate Requester and Approver

Phone Number of the Organization

Internal Email Address or Verified Email Address

Contact Information of the Certificate Approver and Requester

Name and Signature of the Certificate Requester

2) Copies of the Organization ID

Please refer to Section 3.2.2.6 for the applicable IDs.

3) Proofs of the approver and requester's ID[1]（Proofs of the certificate approver's ID are needed only for institution）:

Copies of the certificate requester's ID,

Copies of the approver's ID, and two other proofs. One must be from financial institutions, such as effective credit card, effective debit card, bank statement for a period of no shorter than six months. The other can be phone bill, birth certificate, tax return, social insurance certificate, driver license, passport, etc.

4) Letter of authorization for the certificate requester from the organization;

5) Lawyer opinion letterand lawyer's certificate:

The document signed by alegal consultant proves the existence of the company and a copy of the certificate of the legal consultant.

6) CSR

Except the fifth and sixth items, the materials listed above should bear the corporate seals of the applicants, and should warrant the following:

[1] Approver: he could be the owner、patner、senior manager or senior staff in the organization. On the other hand, he could also be an authorized person carring out the certificate application and usage.

(1) Accuracy of Information;

(2) Protection of Private Key;

(3) Proper Use of EV Certificate;

(4) Revocation upon Compromise;

(5) Acceptance of EV Certificate;

(6) Responsiveness for CFCA's instructions on key comprimises or misuses;

(7) Termination of Use of the Expired EV Certificate.

(8) Acknoledgement and acceptance that CFCA has the right to revoke the certificate under certain conditions.

Please refer to 3.2.2 for detailed information on subscriber's terms of agreement.

8、Verification by CFCA on EV SSL Certificate Request

（1）Verification of Applicant's Identity

- **Focus of Verification of Applicant's Legal Existence and Identity**
  - ✧ Private Organizations: legal existence, formal legal name, registration number, registration agency, EV certificate approver;
  - ✧ Business Entities: legal existence, formal legal name, registration number, EV certificate approver;
  - ✧ Government Agencies: legal existence, formal legal name, registration number;
  - ✧ Non-Commercial Entities: legal existence, formal legal name, registration number.

- **Methods of Verification of Applicant's Legal Existence and Identity**
  - Verify the Certificate of Organization Code on the website of the "National Administration of Code management center"(http://www.nacao.org.cn/).
  - Verify the organization identity through business registration repositories;
  - Verify the organization identity through taxation registration reporsitories;
  - Inqury the superior authority of the applicants;
  - Verify the organization identity using independent and eligible information source.
- **Focus of Verification of the Applicant**
  - The legal existence of the applicant and the fixed place of business should be verified through authoritative third party source.
  - The accuracy of the identity information, including organization name, organizational form, registration number, legal person, registration capital, founding date, annual inspection date, etc.

    CFCA will use necessary methods to verify the capacity of business continuity of the applicant, if it has been set up for no more than three years, and has not been listed in eligible independent information source (e.g. the website of organizational code inquiry) or the government tax information

source (e.g.tax registration certificate). For example, CFCA could request the applicant to supply a bank statement of current account balance.

- **Verification of the Identity of the EV Certificate Request Approver**
  - CFCA must verify the identity of the certificate approver through face-to-face contact and other methods.
  - The certificate approver (for the institution applicant) is required to submit two paper proofs of identity. One is a copy of the approver's ID. Another can be effective credit card, effective debit card, and bank statement for a period of no shorter than six months. The following proofs are also applicable: phone bill, birth certificate, tax return, social insurance certificate, driver license, passport, etc.
  - The investigator of CFCA verifies the certificate approver's ID through the ID repository of the public security bureau, or other authoritative third party reporsitories.
  - The applicant shall issue letters of authorization for the certificate approver and requester. CFCA contacts the authorizer through fix-line telephone (must be verified main phone number of the applicant).Through this, CFCA verifies that the certificate requester and approver have been authorized to apply for and approve the certificate.

- ✧ CFCA contacts the HR department of the applicant through fix-line telephone (must be verified main phone number of the applicant), to verify the name, title and responsibilities of the certificate requester, approver and authorizer.

（2）Verification of the Domain Name

CFCA performs a WHOIS inquiry on the internet for the domain name supplied by the applicant, to verify that the applicant is the entity to whom the domain name is registered. This is an initial verification that the applicant owns the domain name.

If the registration information is confidential, but the domain name registry provides contact with the registered holders, CFCA can contact the registered holders through email or letter via the registry.

In cases where applicant is not the registered holder of the domain name, CFCA will obtain a letter of authorization from the subscriber, or email the resitered holder to inqury whether the applicant has exclusive right to use the domain name. Through this, CFCA can verify that the applicant holds the exclusive right to use the domain name.

（3）CSR Compliance Verification

The CSR is verified to determine whether the CSR and the Certificate Request informationare consistent; whether it’s in line with relevant norms; whether the applicant possesses the private key.

（4）Public Key Delivery for EV SSL Certificate

CFCA issues certificates for subscribers, and deliver the public key certificates to the subscribers via emails.

3.2.2.5 Authentication of the Identities of Other type of Certificate Subscribers

For Code-signing certificates, CFCA would verify the code issuer's identity, address, and country.

For device and VPN certificates, applicants' identity, address, and country are verified.

For Email Certificate, CFCA only issue certificates to domain name email that can be verified through WHOIS. CFCA verifies the validity of the email address and determines whether it's legitimate through appropriate channels including but not limited to verification E-mails.

Standards of verification for identity are the same as listed in 3.2.2.1 and 3.2.2.2 .

3.2.2.6 Applicable IDs

Applicable IDs

Personal ID Types	Organizational ID Types
Resident Identity Card	Business Registration Certificate
Passport	Business License
Military ID	Certificate of Organizational Code

Foreigner's Permanent Residence Permit	Tax Registration Certificate
Social Security Card	Certificate of Legal Person Code
Armed Police ID	Certificate of Public Institution with Legal Person Status
Mainland Pass for Hong Kong and Macao Residents	Registration Certificate of Social Organization
Mainland Pass for Taiwan Residents	Registration Certificate of Private Non-Commerical Entity
Household Register	Registration Certificate of a Foreign Resident Office
Temporary Resident ID	Government Approval
Police （Police Official） Certificate	Others

3.2.3 Non-Verified Subscriber Information

CFCA verifies all the information submitted by the subscribers.

3.2.4 Validation of Authorization

When a person applies for a certificate on behalf of the organization subscriber, enough proofs should be obtained to verify that the person is authorized. CFCA is

obliged to verify that authorization, and store the authorization information.

3.2.5 Criteria for Interoperation

CFCA performs identity verification of the applicants for certificates issued by OCA2 and EV OCA. No other organization is delegated with this function. If another CA is delegated to verify identity of the subscribers, CFCA will carry out re-verification of the identity of subscribers of SSL and EV SSL Certificates. Other situations are not covered by this stipulation.

3.3 Identification and Authentication for Renew Requests

Both “Reissuance” and “Renew” are commonly described as “Certificate Renewal”.

1. Certificate Reissuance

Certificate reissuance is the issuance of a new certificate to the subscriber during the validity period of the certificate.

The subscriber may request for certificate reissuance if:

(1)The subscriber certificate is lost or damaged. For example, the storage media of the certificate is damaged.

(2)The subscriber believes the security of the original certificate and key to be compromised (For example, the subscriber suspects the certificate has been stolen or the private key is attacked).

(3)Other reasons recognized by CFCA.

If a certificate reissuance is necessary, the subscriber should make a certificate reissuance request to CFCA. If this happens within three months following the issuance of the original certificate, the subscriber only needs to re-submit a CSR, no more identity verification materials. CFCA verify subscriber's identity according to the information the subscriber provided in the initial application. CFCA will re-verify the identity of the subscriber if more than three months after the first application. The process and requirements are the same as to the initial request.

Upon the issuance of the new certificate, the original certificate is revoked. The new certificate remains valid for the period between its issuance to the expiry date of the original certificate.

2. Certificate Renew

Certificate renew is the application for the issuance of a new certificate within the three months prior to the expiration of the existing certificate or after the expiration. For Server Certificates, the original certificate is revoked once the new certificate is downloaded successfully. The new certificate is valid between its issuance and the expiry date of the original certificate. This is the same for the other certificates.

The subscriber may request for certificate rekey when the subscriber certificate is about to expire or has expired.

During the three months before the expiry date, CFCA reminds the subscriber to apply for certificate rekey via appropriate channels.

To apply for certificate rekey, the subscriber should appoint a certificate requester and issue a written letter of authorization, provide effective identity proofs and certificate rekey materials, accept the provisions of stated in the Certificate Rekey Request, and agree to bear corresponding responsibility. Upon receiving the Certificate Rekey Request, CFCA will re-verify the authenticity of the subscriber's identity. It will also ensure that the subscriber still owns the domain name of the IP address indentified in the certificate. A new certificate can only be issued after the verification.

When the certificate is rekeyed, the new certificate will remain valid for the period between its issuance to the expiration date of the original certificate and for another validity period (if the rekey is for expired certificate, the new certificate will only be valid for one validity period).

3.3.1 Identification and Authentication for Routine Renew

Same as Section 3.3;

3.3.2 Identification and Authentication for Renew After Revocation

CFCA treats the rekey request after revocation as a new application for certificate, and follows the provisions of Section 3.2.2.

3.4 Certificate Renewal

Certificate renewal is the issuance of a new certificate for an existing key pair. CFCA does not provide certificate renewal service. In other words, when a new certificate is issued, the key pairs must be re-generated

3.5 Identification and Authentication for Revocation Request

The identification and authentication for revocation request follows the procedures stated in Section 4.8.3.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Any entity that needs to use the certificate under the CFCA Global Trust System can raise a certificate request.

4.1.2 Enrollment Process and Responsibilities

1. End-User Certificate Subscribers

End-user certificate subscribers refer to the entity applying for the certificates.

All end-user certificate subscribers shall manifest assent to the CPS and CP (available on the CFCA website) that state the responsibilities and obligations of the subscribers. They shall also submit authentic and accurate application information following the provisions of Section 3.2.2. According to the 《Electronic Signature Law of the People's Republic of China》, if relying parties, CFCA or RA designated by CFCA suffer loss because the application information submitted by the subscriber is unauthentic, incomplete or inaccurate, or because of other wrongful acts of the subscriber, the subscriber shall bear corresponding legal obligation and compensation responsibility. The subscribers are also obliged to keep the private keys safe.

2. CA and RA

CFCA is a CA, and performs some of the functions of RA. For example, the subscriber can submit a certificate request directly to CFCA, who will then reponse to the request and carry out identity verification. Meanwhile, CFCA has authorized banks and some other organizations to accept Certificate Requests in the capacity of RA. RAs verify the identity of the subscribers according to the requirements stated in Section 3.2.2. CFCA and RA issue certificates to subscribers who have undergone the verification. As a CA, CFCA should properly retain subscribers' application documents, archive relevant information at CFCA within appropriate time limit, and practice the responsibilities and obligations stated in this CPS.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

1. At least three trusted roles should be set in the processing of certification application: information collection, information authentication and certificate issuance.

The former two roles can be perfomed by one person, while the last one must be sperated from the former two.

2. For Certificates request, final review of the applicant information should be performed.

1) All the information and documents used to verify the Certificate Request should be reviewed to look for potential conflictive information or information that needs further authentication.

2)If the questions raised by the reviewer need to be futher verified, CFCA must obtain more information and evidences from eligible information sources of the applicant, certificate signer and approver.

3) CFCA must ensure that the information and materials collected regarding the certificate request are adequate to ensure that the Certificate will not contain false information that CFCA is or should be aware of. Otherwise, CFCA will reject the certificate request.

4) If parts of or all of the materials used to verify the subscriber identity are not written in the official language of CFCA, it will appoint properly trained and

experienced personnel with adequate judgement to complete the final cross-correlation and due diligence. This is done by:

4.1) Relying on translation of the materials;

4.2) Relying on RA with competency of the language in question. CFCA will review the authentication results of the RA and ensure that the self-assessment requirements in the Certificate standards are met.

3. If CFCA delegates another organization to perform the functions of RA, CFCA is responsible for the final review of the certificate request verified by the RA.

4.2.2 Approval or Rejection of Certificate Applications

CFCA will approve a certificate request if all application materials and identity information have been verified in terms of Section 3.2.2. Otherwise, CFCA will reject the request and timely notice the applicant of the result and the reasons.

4.2.3 Time to Process Certificate Applications

CFCA will complete the processing of certificate requests within a reasonable time. If application materials are complete and in line with the requirements, the request will be processed within 1-3 working day. EV SSL Certificate request will be processed within five working days, or within ten days in special circumstances.

4.3 Certificate Issuance

4.3.1 CA and RA Actions during Certificate Issuance

A certificate is created and issued following the approval of a certificate application by CFCA or following receipt of an RA's request to issue the certificate. CFCA creates and issues to a certificate applicant a certificate based on the information in a certificate application following approval of such certificate application.

4.3.2 Notifications to Subscriber by the CA and RA of Issuance of Certificate

CFCA is obliged to notice the subscriber of the results of the certificate request, whether it's approved or rejected. CFCA can do so via phone, email or other channels.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conducts constitute the subscriber's acceptance of the certificate: filling in the certificate request form, agreeing to the stipulations in this CPS, providing authentic and accurate identity information which is successfully verified by CFCA, and receiving the certificate issued by CFCA. After receiving the certificate, the subscriber should verify the information contained in the

certificate before use. If no comments are raised within one working day, it is considered as the subscriber has accepted the certificate.

4.4.2 Publication of the Certificate by the CA

For end-user subscriber certificate, CFCA will publicize the certificate in due form according to the opinion of the subscriber. CFCA will not publicize the end-user subscriber certificate if the subscriber has not requested it to do so.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

CFCA does not notice the other entity about the certificates it issued. Relying parties may access the certificates in the repositories.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Private key and certificate use shall be consistent with the predetermined and approved usages (refer to Section 1.4.1). The subscribers shall follow this CPS in terms of certificate use, and shall protect their private keys to avoid unauthorized use.

1、 Private Key and Certificate Use by the Subscriber

The subscribers shall only use the private keys when they have accepted the corresponding certificates, shall only use the private keys and certificates in

intended functions, and shall cease to use the certificates and private keys when the certificates expire or are revoked. For Pre-Generated Certificates, they and their corresponding private keys shall only be used after the certificates have been activated.

2、 Public Key and Certificate Use by Relying Parties

When the relying parties receive signature information, they shall:

- ✧ Obtain the corresponding certificates and certificate chains;
- ✧ Assess the validity of the certificates;
- ✧ Make sure that the certificates corresponding to the signatures are trusted by the relying parties;
- ✧ Verify that one of the intended usages of the certificates is signing;
- ✧ Perform signature verification using the public keys on the certificates.

If relying parties fail to perform any of the above actions, they should reject to signatures.

When relying parties need to send encrypted information to the receiving parties, they should first obtain the encryption certificates of the receiving parties through proper channels, and use the public keys on the certificates to encrypt the information.

4.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance on the trust relationship proved by the certificates issued by the CFCA Global Trust System, relying parties shall:

1. Obtain and install the certificate chains corresponding to the certificates;

2. Verify that the certificates are valid. To do so, relying parties need to obtain the latest CRL released by the CFCA to ensure that the certificates have not been revoked. All the certificates appear in the certificate pathes should be assess on their reliability. Validity period of the certificates shall be checked. Relying parties should also review other information that may affect the validity of the certificates.

3. Make sure that the content on the certificates is consistent with the content to be proved.

4.6 Certificate Rekey

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key.

4.6.1 Circumstances for Certificate Rekey

1. When the subscriber certificate is about to expire or has expired;

2. When the private key has been compromised;

3. When the subscriber knows or suspects that the certificate or private key has been compromised;

4. When the other situations that necessitate certificate rekey happens.

4.6.2 Who May Request Rekey

Subscribers holding certificates issued by CFCA may request certificate rekey.

4.6.3 Processing Certificate Rekey Requests

Same as Section 3.3;

4.6.4 Notification of New Certificate Issuance to Subscriber

Same as Section 4.3.2;

4.6.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Same as Section 4.4.1;

4.6.6 Publication of the Rekeyed Certificate by the CA

Same as Section 4.4.2;

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Same as Section 4.4.3;

4.7 Certificate Modification

No certificate modification service is provided by CFCA.

4.8 Certificate Revocation and Suspension

4.8.1 Circumstances for Revocation

CFCA will revoke a certificate it has issued upon the occurrence of any of the following events:

1. The Subscriber requests in writing that the CFCA revoke the Certificate;

2. The Subscriber notifies the CFCA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The CFCA 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 technical requirements ;

4. The CFCA obtains evidence that the Certificate was misused;

5. The CFCA is made aware that a Subscriber has violated one or more of its material obligations under theSubscriber or Terms of Use Agreement;

6. The CFCA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a DomainName Registrant's right to use the Domain Name, a relevant licensing or services agreement between theDomain Name Registrant and the Applicant has

terminated, or the Domain Name Registrant has failed to renew the Domain Name);

7. The CFCA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

8. The CFCA is made aware of a material change in the information contained in the Certificate;

9. The CFCA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;

10. The CFCA determines that any of the information appearing in the Certificate is inaccurate or misleading;

11. The CFCA ceases operations for any reason and has not made arrangements for another CA to provide

revocation support for the Certificate;

12. The CFCA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CFCA has made arrangements to continue maintaining the CRL/OCSP Repository;

13. The CFCA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;

14. Revocation is required by the CFCA's Certificate Policy and/or Certification Practice Statement;

15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CFCA within a given period of time).

16. Other situations stipulated in relevant laws and regulations.

.

4.8.2 Who Can Request Revocation

All subscribers holding CFCA certificates can request revocation.

At the same time, CFCA can take the initiative to revoke a subscriber certificate if an event described in Section 4.8.1 occurs.

4.8.3 Procedure for Revocation Request

Revocation includes initiative revocation and reactive revocation. Initiative revocation refers to one that put forward by the subscriber, reviewed and performed by CFCA. Reactive revocation refers to one that CFCA initiated to terminate trust services for the certificate, the usage of which has violated relevant regulations and agreements, or the subject of which has exincted.

4.8.3.1 Initiative Revocation

Before the subscriber applies for certificate, it should appoint a requester and provide a written letter of authorization, provide effective identity proofs, accept relevant provisions, and agree to bear corresponding responsibilities.

Upon receiving the application, CFCA should verify whether the certificate implied is issued by CFCA, is valid, and that the reason for revocation is true. If these verifications come up with satisfactory results, CFCA will perform the revocation.

4.8.3.2 Reactive Revocation

When reactive revocation is planned, CFCA shall inform the subscriber through appropriate channels of the certificate in question, reason and time limit for revocation. CFCA shall only revoke the certificate when it ensures that the subscriber is informed and consents to the revocation.

4.8.4 Revocation Request Grace Period

For initiative revocation, the subscriber should make the request as soon as they identity such a need.

For reactive revocation, the subscriber can submit their arguments within three working days upon receiving the notice. CFCA will assess the arguments. If the arguments are justifiable, the revocation will be redrawed. If the subscriber doesn’t response within three working days, or reply that they agree with the revocation, CFCA will go ahead with the revocation.

4.8.5 Time within Which CA Must Process the Revocation Request

For initiative revocation, it will be performed within 24 hours after the revocation request is reviewed.

For reactive revocation, the subscriber can submit their arguments within three working days upon receiving the notice. CFCA will assess the arguments. If the arguments are justifiable, the revocation will be redrawed. If the subscriber doesn't response within three working days, or reply that they agree with the revocation, CFCA will perform the revocation within 24 hours.

4.8.6 Revocation Checking Requirements for Relying Parties

Before any act of reliance, the relying parties shall verify that the certificate has not been revoked.

4.8.7 CRL Issuance Frequency

CFCA differentiate CRL updating according to the systems that issue the certificates. CRL information issued by OCA2 and EV OCA will be updated within 24 hours; while that by OCA21 within three hours. The frequency of CRL publication can be tailored according to the demands of the Subscribers. Manual real-time publication of CRL is also applicable if needed.

4.8.8 Maximum Latency for CRLs

The maximum latency fo CRL publication is 24 hours.

4.8.9 Online Revocation/Status Checking Availability

OCSP service is avaible for 7X24.

Whether to proferm an OCSP inquiry depends completely on the security demands of the relying parties. For applications that high demand on security and completely rely on the certificates for identity authentication and authorization, the inquiry should be performed before any act of reliance.

The OCSP service of CFCA follows the RFC2560 standard.

Clients can access the OCSP service through http protocol. CFCA will review the inquiry and focus on the following:

- Verify whether signature is compulsory;
- Verify the signature using CA Certificate;
- Verify whether the certificate is valid or expired;
- Verify whether the sponsor of the certificate is within the list of trusted certificates.

OCSP response should contain the following fields and content:

Field	Value/ Value Restriction
Status	Response status, including success, mal formed

	request, internal error, try later, sig required, and unauthorized. When the response status is success, following information should be shown.
Version	V1
Signature Algorithm	Algorithm used to sign the OCSP, including sha1RSA, sha256RSA and SM3 SM2.
Issuer	The entity that issue the OCSP. Information includes the data value of the issuer's public key and certificate DN.
Response Time	The time that the OCSP response generates.
Certificate Status List	A list that contains the status of the certificates. The status includes certificate identifier, certificate status, and certificate revocation.
Certificate Identifier	Including the data digest algorithm, data value of the certificate DN, the data value of the public key, and certificate serial value.
Certificate Status	Latest status of the certificate, including "good", "revoked" and "unknown".
Certificate Revocation	Revocation time and reason if the returned

	status is “revoked”.

The extensions of OCSP are consistent with that stated in RFC2560 standard.

The OSCP is updated within 24 hours, and the maximum service reponse is less than 10 seconds. The maximum validity period for OCSP response does not exceed 7 days.

4.8.10 Other Forms of Revocation Advertisements Available

Information on certificate revocation is made available through CRL or OCSP services. CRL information can be obtained from the CRL Address extension.

4.8.11 Special Requirements regarding Key Compromise

If the subscriber discovers or has adequate reasons to believe that the security of the private key is threated, it should make a revocation request as soon as possible.

4.8.12 Certificate Suspension

Not applicable for the certificates under the Global Trust System.

4.9 Certificate Status Services

4.9.1 Operational Characteristics

Certificate status is available through the OCSP service of CFCA.

4.9.2 Service Availability

Certificate status inquiry service is provided 7X24 by the CFCA.

4.10 End of Subscription

The subscription is ened when：

1. The certificate has expired;
2. The certificate is revoked.

4.11 Key Generation, Backup and Recovery

To ensure the security of subscriber private keys, subscribers should independently perform key pair generation in a secure environment and store the encrypted keys in secure media. The subscribers should backup the keys in a timely manner, and prevent the keys from loss. During the period after key pair generation and Server Certificate installation, the subscribers should not change any configuration of the servers, so as to prevent loss of the keys. The subscribers should apply for certificate rekey once key leakage is known or suspected.

When the subscribers delegate other trustworthy service suppliers to perform key generation for them, they shall require the suppliers to bear confidentiality responsibilities.

5 CA Facility, Management, and Operational Controls

5.1 Physical Controls

Physical and environmental securities of the systems constitute the foundation of the security of entire CFCA system. Physical and environmental controls include infrastructure management, monitoring of the environment, area access control, device security and disaster prevention, etc. The CFCA system is placed in a safe and robust building, and possesses independent software and hardware operation environment. The site selection has fully considered threats, such as water hazards, fire, earthquakes, electromagnetic disruption, radiation, criminal activities and industrial accidents.

5.1.1 Site Location and Construction

The computer room of the CFCA CA system is located in the No.2 Building (China UnionPay Beijing Information Center), Zhongguancun Software Park, Haidian District, Beijing. Access to the computer room is subjected to a three-layer control. The electromagnetic shielding of the computer room meets the Level “C” requirements of the GJBz20219－94 Standard. The computer room is built to prevent and minimize the impacts of earthquakes, fire and water exposures. The computer room is equipped with temperature and humidity control devices,

independent power supply, back-up power generator, access control and camera monitors. These security measures can ensure the continuity and reliability of the certification services.

5.1.2 Physical Access

Vistors are subjected to the authentication of the China UnionPay Beijing Information Center and CFCA and need to go through two layers of access control before they enter into the office area of CFCA. They are also accompynied by CFCA employees.

The access to the comprehensive computer room by operators is controlled by fingerprint authentication and access card authentication, and is monitored by cameras 7*24.

The access to the restricted computer room by operators is controlled by three layers of security controls: the dual person fingerprint authentication, access card authentication, and dual person access card authentication. The entry and exit of the restricted computer room are recorded in the security system of the monitor room.

5.1.3 Power and Air Conditioning

Two sets of three UPSs supply the power for the computer room. As a result, the power supply for the systems can last for over 30 minutes even if one of the UPSs breakdown. A disel generator has been put in place to strengthen the power

supply stability of the systems. It can be used to power the UPS when the external power supply is cut off.

The computer room is equipped with multiple central air conditioners and ventilation devices to ensure that the temperature and humidity meet the national standards: GBJ19-87 Standards on Heating, Ventilation and Air-Conditioning Design, GB50174-93 Standards on Computer Room Design.

5.1.4 Water Exposures

CFCA employs professional technical measures to prevent and detect water leakage, and is able to minimize the impact of water leakage on the certification systems.

5.1.5 Fire Prevention and Protection

The CFCA computer room is built of fire-proof materials, and is equipped with central fire monitors and automatic gaseous media fire-extinguishing systems. It has undergone the checking of a national authority which proves that it can effectively lower fire threat.

5.1.6 Media Storage

CFCA has formulated control policies for the management of the storage media of important data. The purpose is to prevent the leakage of important information, intentional compromise and damage.

5.1.7 Waste Disposal

Files (including paper files, disks and floppy disks, etc) containing sensitive information should be shredded before disposal. Media must be rendered unreadable before disposal. Media containing confidential information should be zerorized in accordance with the guidance of the manufacturers. Cryptograhic devices and other important key devices are disposed according to the management methods of cryptographic devices.

5.1.8 Off-Site Backup

CFCA has set up a mechanism for same-city off-site backup of core data.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles of CFCA include:

Customer service personnel

Security personnel

Key and cryptographic device management personnel

Cryptographic device operation personnel

System administration personnel

Human resources management personnel

5.2.2 Number of Persons Required per Task

CFCA has established rigorous policies to ensure segregation of duties based on job responsibilities. Sensitive tasks, such as the access to and management of CA cryptographic hardware and associated key require three trusted persons.

At least two trusted persons are required to perform other operations, such as certificate issuance.

Policies and procedures are in place to ensure clear segregation of duties for its employees who can balance each other's power and monitor each other.

5.2.3 Identification and Authentication for Each Role

Before employing a trusted role, CFCA performs background check according to the stipulation in Section 5.3.2.

CFCA uses access card and fingerprint verifications to control physical access. It also determines the access rights of the personnel.

CFCA use digital certification and user name/key to identify and verify trusted roles. The system holds independent and complete record of all operations.

5.2.4 Roles Requiring Seperation of Duties

Roles requiring segregation of duties include (but are not limited to):

Security personnel, sytem administration personnel, network management personnel, operators

Subscriber information collection personnel, subscriber identity and

information verification personnel, RA information input personnel, RA certificate generation personnel.

5.3 Personnel Controls

CFCA and its RAs should follow the following requirements to manage staff members.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking to become trusted roles must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities, as well as proof of any government clearance.

5.3.2 Background Check Procedures

Prior to commencement of employment of a trusted role, CFCA conducts background checks which include the following procedures:

(1)The applicants submit required materials.

They are required to submit valid proof of their working experience, highest educational degree obtained, qualifications and ID, etc.

(2) CFCA verifies the identities of the applicants.

CFCA HR department would authenticate the submitted materials through phone calls, letters, internet, face-to-face interviews, and reading of archives.

(3)The applicants undergo a three-month probation period.

CFCA would ask the applicants to take exams and scenarios tests, and would observe the performance of the applicants.

The results of the abovesaid exams, tests and observation should meet the requirement stipulated in Section 5.3.1.

(4)The new employees sign confidentially agreements.

CFCA requires the new employees to sign confidentially agreements.

(5)The employement is commenced.

5.3.3 Training Requirements

CFCA provides ite employees with trainings upon hire. The trainings are arranged according to the job responsibilities and roles of the employees and cover the following topics: PKI concpets, job responsibilities, internal policies and procedures, certification systems and softwares, relevant applications, operation systems, network, ISO9000 quality control mechanism and CPS, etc.

Employees handling Certificate related business must be trained according to the following:

1) Employees responsible for information and identity verification (verification experts) are trained on: basic PKI concepts, validation and verification policies and procedures, major threats during the verification (e.g. network phishing and other social engineering techniques) and EV certificate standards.

2) Training records should be kept and ensure that verification experts meet the

technical demands of their jobs.

3) Different certificate issuance rights should be given to the verification experts according to their levels of technical skills. The grading standards of technicial skills should be aligned with the training content and performance evaluation criteria.

4) Before designation of certificate issuance rights, CFCA should make sure all the verification experts of different technical levels are competent of their jobs.

5) All verification experts should be required to pass the internal examination on identity verification of certificates.

5.3.4 Retraining Frequency and Requirements

CFCA provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

CFCA determines and arranges job rotation frequency and sequence according to the situations.

5.3.6 Sanctions for Unauthorized Actions

Employees who have taken unauthorized actions would be suspended from their jobs and subjected to disciplinary punishements according to relevant

administration policies and procedures.

5.3.7 Independent Contractor Requirements

Personnel seeking to become the independent contractors of CFCA need to provide valid proof of ID, diplomas and qualifications, and sign confidentiality agreements with CFCA before the commencement of their employment.

5.3.8 Documentation Supplied to Personnel

CFCA provides its employees the requisite documents needed to perform their job responsibilities.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Loggs include but are not limited to the following six types:

1. CA key life cycle management events, including key generation, backup, recovery, archival and destruction;

2. The indentity information of the Subscribers recorded in the RA system.

3. Certificate life cycle management events, including certificate requests, rekey and revocation;

4. System and network security records, including the record of the instruder detection system, logs generates during system daily operations, system problem handling forms, system change forms and etc;

5. Access control records;

6. System inspection records.

Log entries include the following elements: date and time of the entry; serial or sequence number of entry; identity of the entity making the journal entry;kind of entry.

5.4.2 Frequency of Processing Log

Type one logs listed above are collected and managed by the key administraters; type two and three are recorded by the database and undergo incremental backup daily, and weekly full backup; type four logs are automatically stored on backup devices daily; type five logs are audited quarterly; type six logs are checked daily.

5.4.3 Retention Period for Audit Log

Audit logs related to certificates shall be retained for at least ten years following the date the certificate expires or is revoked.

5.4.4 Protection of Audit Log

Management policies have been established, while logical and physical controls are in place to restrict operation on audit logs to authorized personnel. The audit logs are under strict protection which fends off any unauthorized manipulation.

5.4.5 Audit Log Backup Procedures

The backup of system, database and transaction logs follows CFCA's Log Management Method and Data Backup Management Methods.

5.4.6 Audit Collection System

Applications, network and operation systems automatically generate audit data and records.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual and organization that caused the event.

5.4.8 Vulnerability Assessments

Using audit logs, vulnerability assessments are periodically on system, physical facilities, operation management, human resources management and other aspects. Actions are taken according to the assessment reports.

5.5 Records Archival

5.5.1 Types of Records Archived

Besides the records stated in Section 5.4.1, CFCA archives:

1. Application documents, identity verification documents, Agreements signed

with Subscribers, Subscriber certificates and CRL;

2. CPS, CP and management policies;

3. Employee materials, including employee information, background check document, training, employment and resignation records;

4. Internal and external assessment documents.

5.5.2 Retention Period for Archive

CFCA would retain all archived documents for 10 years after the expiry of corresponding certificates.

If required by laws, CFCA shall extend the record retain periods.

The certificate revocation records on CRL and OCSP shall not be deleted during the valid period of the certificate.

5.5.3 Protection of Archive

CFCA has made policies to protect the archives.

For electronic archives, only authorized trusted persons are able to obtain access to them. The archives are protected against unauthorized viewing, modification, deletion, or other tampering during their retention period. To this end, CFCA uses reliable storage media and archive processing applications.

For paper archives, CFCA has made corresponding management methods, and has appointed dedicated libarian to managed the archives. Policie have been formulated to restrict the access to the paper arhives to authorized personnel.

5.5.4 Archive Backup Procedures

Database, operation systems, CRL records and logs are backuped.

Database backup: local and offsite backup, incremental and full backup.

Operation system backup: Backup performed at when the operation system is launched and when there are system changes.

CRL backup: Files are automatically transmitted from FTP to the backup server daily. Manual checks are performed to ensure successful transmission.

5.5.5 Requirements for Time-Stamping of Records

Archives shall contain time and date information. Time and date information shall be added to system generated records according to standards.

5.5.6 Archive Collection System

CFCA has put in place an automatic archive collection system.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized trusted persons can have access to arhives. When archives are restored, they should be checked for completeness.

5.6 Key Changeover

CA key pairs are retired from service at the end of their respective accumulative maximum lifetime as defined in Section 6.3.2. Key changeover

unfolds according to the following procedures:

A superior CA should cease to issue new subordinate CA certificates no later than 60 days before the expiry date of its private key (Stop Issuance Date).

Generatie a new key pair, and issue a new superior CA certificate.

Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the “Stop Issuance Date,” Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CFCA has established a business continuity plan (BCP). It provides guidance to actions when CFCA is attacked or undergoes communication or network breakdown, computers and devices do not function normally, software is compromised, and when database is tampered.

The BCP is the responsibility of the CFCA Operation Security Committee (Security Committee for short), who’s functions include direct and manage information security, approve and release BCPs, launch disaster recovery, etc. The

Security Committee is made of leaders and the department heads, and is headed by the General Manager.

Business interruption is classified as emergencies and disaterous events. Emergencies are interruptions with major impacts on services to the client, but the service resumption is not affected by external factors and can be achieved with a short period of time. Disaterous events are interruptions caused by force majeure, such as natural disasters, contagious disease, and political outbreaks, etc.

CFCA has formulated corresponding emergency procedures for emergencies and disaterous events.

When emergency happens, the head of the Security Committee will convene a meeting of the members to evaluate the interruption. The operation department will perform the predetermined procedures. Meanwhile, the marketing department and technical support department will properly handle the affected clients. Afterward, CFCA will evaluate the effectiveness of the risk prevention measures and improve on them.

When a disaterous event happens, it will be handled according to the stipulations stated in Section 5.7.4.

As to normal breakdowns, it will be resolved within two hours; emergencies, 24 hours. As to disaterous events, if normal operations are not possible at the main site for disasters or other force majeure, certification services will be resumed within 48 hours at the backup site using backup data and devices.

Dedicated problem reporting and response capacity have been designated for

SSL certificates:

1)CFCA provides subscribers, relying parties, application software vendors, and other third parties with clear guidance to report complaints or suspected private key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates ("Certificate Problem Reports"), and a 24x7 capability to accept and acknowledge such Reports;

2)CFCA will begin investigation of all Certificate Problem Reports within twenty-four (24) business hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

(i) The nature of the alleged problem;

(ii) Number of Certificate Problem Reports received about a particular Certificate or website;

(iii) The identity of the complainants; and

(iv) Relevant legislation in force.

3) CFCA takes reasonable steps to provide continuous 24/7 ability to internally respond to any high priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an Certificate that is the subject of such a complaint.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

In the event of the corruption of computing resources, software, and/or data,

such an occurance is classified according to the stipulations in Section 5.7.1 and is acted upon according to its classification.

5.7.3 Entity Private Key Compromise Procedures

CFCA has formulated an emergency plan on root private key leakage, which clearly stipulates the internal processing procedures, responsibilities of personnel and the procedures of external communication.

Once a root private key leakage is confirmed, CFCA will report to the competent department regarding the time, cause of the leakage and corrective actions.

Once a root private key leakage is confirmed, the subscribers and relying parties will be noticed immediately. All the certificates will be revoked. No new certificate will be signed with the private key.

5.7.4 Business Continuity Capabilities after a Disaster

CFCA has set up a data backup center and a corresponding BCP to ensure business conitinuity after a disaster.

If normal operations are not possible at the main site for disasters or other force majeure, certification services will be resumed within 48 hours at the backup site using backup data and devices.

5.8 CA or RA Termination

When CFCA plans to terminate certification services, it will report to the competent department sixty days in advance, and go through the procedures of cancelling certification qualification.

When CFCA plans to suspend or terminate certification services, it will take the following actions ninety days in advance:

Notice the RA, subscribers, relying parties and other parties about continuation of the services;

Compensate the RA according to the cooperative agreement;

Compensate the subscribers and relying parties according to the service agreements;

Provide the business undertaker with the following and more information: certificate transaction materials, certificate repository, and latest certificate status information.

CFCA will report to the competent department about the suspension or teminaiton of its certification services sixty days in advance, and will make arrangement with the business undertaker.

If CFCA fails to reach an agreement with the other certification service organization about busiess transfer, it can request the competent department to arrange one.

If the competent department has regulations in this aspect, those regulations should be followed strictly.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

1. CA Signing Key Generation

CA signing key generation is performed within the cryptographic device meeting the requirements of the state cryptography administration. The cryptographic device uses split ownership (secret share) and secret sharing mechanism to backup the key pairs, the fragments of which are held by shareholders (the custodians of the key fragments). The key generation ceremony is performed strictly according to the management methods of cryptographic devices and keys. Five persons are selected and authorized as the custodians, who use the passwords they input to protect the key fragments they are entrusted with. The key fragments are stored in smart IC cards. The CA key generation occurs in the area with the highest security level. Three out of the five custodians perform the ceremony which is monitored by a third party auditor. The CA key generation, storage and password cryptographic modules should meet the requirements of the state cryptography administration.

2. RA Key Generation

Generation of RA key pairs is performed under security controls. The RA certificates are issued by CFCA.

3. Subscriber Key Generation

Generation of subscriber key pairs is performed by the subscribers. They should ensure the reliability of the key pairs and is responsible for protecting the private key, and bears corresponding legal obligations.

Generation of key pairs of pre-generated certificates is performed by authorized personnel. Stringent policies have been made to ensure the security of key pairs when the certificates are delivered to the subscribers.

CFCA is obliged to provide guidance to the subscribers to perform key generation according to correct procedures. CFCA would reject a certificate application with weak keys. When needed, it can designate technical personnel to assist the subscribers in key generation.

Parties other than the subscriber should not archive subscriber's private key.

If CFCA or its RAs obtains the evidence that the private key is communicated to unauthorized parties, CFCA will revoke the public key certificate corresponding to the compromised private key according to relevant standards.

6.1.2 Private Key Delivery to Subscriber

When end-user subscriber key pairs are generated by the end-user subscriber, private key delivery to a subscriber is not applicable.

For pre-generated certificates, the USBKey used should be approved by the State Cryptographic Administration. The manaufacturer is responsible for the logical security of the USBKey, and shall not write any irrelevant executable code or program in it. The USBKey used by CFCA is blank. Subscriber private key generated by CFCA is delivered safely to the RA, who is responsible for keeping the key safe until it is delivered to the subscriber. Technologies have been employed to make sure that the subscriber private key generated using USBKey cannot be exported.

6.1.3 Public Key Delivery to Certificate Issuer

When applying for server certificates, the subscribers generate key pairs on their servers and submit the public key to CFCA as part of the CSR through emails.

6.1.4 CA Public Key Delivery to Relying Parties

CA public key that can be used to verify the signature of CFCA is available in the repository.

6.1.5 Key Sizes

As to key sizes, CFCA follows the explicit regulations and requirements made by the judicial authorities and the competent department.

Following are the current key sizes and algorithms of the CA signing keys under the Global Trust System:

CFCA GT CA---RSA-2048/SHA-256、SM2-256/SM3；

CFCA GT OCA2—RSA-2048/SHA-256、SM2-256/SM3

CFCA GT OCA21—RSA-2048/SHA-256、SM2-256/SM3

CFCA EV ROOT—RSA-4096/SHA-256、SM2-256/SM3

CFCA EV OCA-RSA-2048/SHA-256、SM2-256/SM3

The key size of subscriber keys is RSA-2048 or SM2-256.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters are generated by cryptographic devices approved by the state cryptography administration. The device should possess the credentials issued by the state cryptography administration.The devices should meet the requirements stated in the Specification of Cryptography and Related Security Technology for Certificate Authentication System released by the State Cryptography Administration and other relevant standards and requirements. An example is the quality inspection standard of public key parameters.The built-in protocols and algorithms of the devices should be of satisfactory security levels.

6.1.7 Key Usage Purposes

CA private key is used to sign its certificate, subordinate CA certificate, subscriber certificate and CRL. CA public key is used to verify the signature of private keys. The usages of subscriber keys are as follow:

Certificate Type	Algorithm	Key Size	Maximum Lifetime (Year)	Key Usage	Extended Key Usage
SSL Certificate	RSA-2048/SHA256 SM2/SM3	RSA-2048、Sm2-256	3	Digital signature, Non-repudiation, Key agreement, Key encrypherment	Server authentication
EV-SSL Certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	2	Digital signature, Non-repudiation, Key agreement, Key encrypherment	Server authentication
VPN Certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	5	Digital signature, Non-repudiation, Key agreement, Key encrypherment, Data encrypherment	Server authentication
Code Signing Certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	5	Digital signature, Non-repudiation	Code signing
Email Certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	3	Digital signature, Non-repudiation, Key agreement, Key encrypherment, Data encrypherment	Server authentication

Device Certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	5	Digital signature, Non-repudiation, Key agreement, Key encrypherment, Data encrypherment	Server authentication
Individual Certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	5	Digital signature, Non-repudiation, Key agreement, Key encrypherment,	Client authentication
Advanced Individual Certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	5	Signing certificate: Digital signature, Non-repudiation, Key agreement, Key encrypherment, Encryption certificate: Key encrypherment, Data encrypherment	Client authentication
Corporate certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	5	Digital signature, Non-repudiation, Key agreement, Key encrypherment,	Client authentication
Advanced Corporate certificate	RSA-2048/SHA1 SM2/SM3	RSA-2048、Sm2-256	5	Signing certificate: Digital signature, Non-repudiation, Key agreement, Key	Client authentication

				encrypherment, Encryption certificate: Key encrypherment, Data encrypherment	

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The cryptographic module (cryptographic device) used for key generation is placed at the core area of CFCA. The module uses high speed host device with complete independent IPR, and is tested and approved by the state cryptography administration. Public key algorithms, like RSA, DSA, SM2, Diffe Hellman, can be used. Optional RSA sizes include 2048 and 4096 bits. Compatible symmetric algorithms include SDBI, DES, TRIPLE-DES, IDEA, RC2, RC4, RC5, SM1, SM4. Strong encryption of 128 bits is supported. Compatible HASH algorithms include MD2, MD5, SHA1, SDHI, SHA256 and SM3.

The public key algorithms for the cryptographic devices used in the CFCA Global Trust System include RSA-2048, RSA-4096, SM2-256; and HASH algorithms include SHA-256 and SM3. The devices have been granted credentials by the State Cryptography Administration.

CFCA has formulated management methods of cryptographic devices, which enable normative approval and management of the whole process of cyrpotgraphic

device usage, including procurement, check and acceptance, installation in the computer room, initialization, activation, usage, backup, maintenance and destruction. The cryptographic devices are linked only to and directly with the application systems, and are sotraged in shielding computer rooms.

6.2.2 Private Key (n out of m) Multi-Person Control

CFCA CA keys are stored in the cryptographic devices, the keys of which are splitted into five fragments that stored in five IC cards. Each of the IC cards is hold by one authorized security personnel (shareholders), and stored in the safes in the shielding computer rooms in the area of the highest security level. The activation of the CA private key requires the present of the three shareholders out of the five. This ensures the security of sensitive operations through technologies and policies.

6.2.3 Private Key Escrow

CA private keys are not escrowed.

6.2.4 Private Key Backup

The CA private keys are generated in cryptographic devices with dual backups. The cryptographic devices are stored in environment that prevents high temperature, high humidity and maganetic affects. The backup operation of the cryptographic devices requires the present of at least three (including three) operators.

The subscriber private keys are generated by the subscribers, who are recommended to backup the keys, and protect the backups by using passwords and other access controls. The purpose is to prevent unauthorized edit or leakage.

6.2.5 Private Key Archival

Upon expiration of the CFCA CA key pairs, they will be securely retained for a period of at least ten years using hardware cryptographic modules described in Section 6.2.1. These CA key pairs are prevented by the CFCA key management policies and procedures to be used in any production system. At the end of the archival periods, CFCA will destroy the key pairs according to the methods stated in Section 6.2.10.

.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CFCA generates CA key pairs on the hardware cryptographic modules. In addition, CFCA has eastablished backup cryptographic devices. Backup CA key pairs are transported off-line in encrypted form.

Subscriber private keys generated by hardware cannot be exported from the cryptographic modules. The subscriber private keys generated in the other ways can be exported in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

The private keys are stored in hardware cryptographic modules as encrypted key fragments as cipher-text.

6.2.8 Method of Activating Private Key

1. Activation of Subscriber Private Key

If the subscriber private key is generated and stored by software, it's stored in the software cryptographic module of the application and protected by passwords. When the application is started up, the software cryptographic module is loaded. Once the module has verified the passwords, the subscriber private key is activated.

When the subscriber private key is generated and stored by hardware cryptographic module, it's protected by the passwords (or pin code) of the hardware. When the cryptographic module is loaded, and verifies the passwords, the subscriber private key is activated.

2. Activation of CA Private Key

CFCA uses hardware (cryptographic devices) to generate and store CA private key. The activation data is splitted according to the provisions stated in Section 6.2.2. Once the CA private key is activated, it will stay activated until the CA log off.

6.2.9 Method of Deactivating Private Key

The subscriber private key is deactivated upon application termination, system log off or power-off of the system.

The CA private key is deactivated upon power-off or re-initialization of the hardware cryptographic module.

6.2.10 Method of Destroying Private Key

Where required, CFCA will archive the CA private key according to the provisions stated in Section 6.2.5. The other CA private key backups will be destroyed in a secure manner. At the end of the archival period, the archived private key will be destroyed when at least three trusted personnel are presented.

The subscriber private key should be destructed after authorization. At the end of the life cycle of the private key, all corresponding key copies and fragments should be destroyed.

6.2.11 Cryptographic Module Rating

CFCA uses high speed host cryptographic devices with complete independent IPR that have been certified and approved by the State Cryptography Administration.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The archival of public keys follows the same requirements as that of certificates, including requirements on retention period, storage and security measurses. Please refer to Section 5.5 for the requirements.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period of CA certificates is 30 years. The validity period of subscriber certificates issued by CFCA is one to five years; while that of EV certificates is two years.

CFCA currently issues certificates with a maximum validity period of 60 months. Beyond 1 April 2015, CFCA only issue certificates with a maximum validity period of 39 months except the following situations:

Beyond 1 April 2015, CFCA MAY continue to issue Subscriber Certificates with a Validity Period greater than 39 months but not greater than 60 months provided that the CFCA documents that the Certificate is for a system or software that:

(a) was in use prior to the Effective Date;

(b) is currently in use by either the Applicant or a substantial number of Relying Parties;

(c) fails to operate if the Validity Period is shorter than 60 months;

(d) Does not contain known security risks to Relying Parties; and

(e) is difficult to patch or replace without substantial economic outlay.

The operational period for key pairs is the same as that for associated certificates. However, the public keys of signing certificates may continue to be used for verification of signatures generated during the validity period of the certificates. This is so until the private keys are compromised, or the key pairs are at risk of decryption. An example of such risks is the decryption of encryption algorithm. For encryption certificates, the private key may continue to be used to ensure successful decryption of information encrypted during the validity period of the certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

1. The generation of CA private key follows the requirements stated in Section 6.2.2.
2. For subscribers, the activation data is the passwords that protect the private keys. For subscribers of pre-generated certificates, the activation data contains the binding identity information. CFCA recommends the subscribers to select strong passwords to protect their private keys.

- The passwords need to contain at least six characters.
- Subscribers are recommended not to use information that can be easily guessed or decrypted, such as birthday or simple and repeated numbers.

6.4.2 Activation Data Protection

1. CFCA shareholders are required to safeguard their secret shares and sign an agreement acknowledging their shareholder responsibilities.

2. The RA is required to store their Administrator/RA private keys in encrypted form using password protection.

3. Subscribers are required to store their private keys in encrypted forms and are recommended to protect their private keys by using double-factor verification (e.g. hardware and strong password).

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

The cryptographic devices and related IC cards containing CA private keys are usually stored in the area with the highest security level, and are not allowed to be taken out of CFCA. If special circumstances necessitate the transmission, it should be witnessed by the security personnel and shareholders.

The passwords for private key activation transported through networks should be in encrypted forms to prevent loss. For the activation data of

Pre-Generated Certificate, CFCA will verify the completeness of the data and the validity of the signature.

6.4.3.2 Activation Data Destruction

CFCA destroys the activation data of CA private key by device initialization.

When the activation data of subscriber private key is no longer needed, it shall be destroyed. The subscriber should make sure that no other party can restore the data directly or indirectly through the residual information or the storage media.

6.5 Data Security Controls

6.5.1 A Security Plan made for Data Protection

1. CFCA adopts access controls and encryption signature to: ensure controls on CA; protect the confidentiality, completeness and serviceability of the data relating to certificate request, and the procedures relating to Certificate; restrict access, usage, disclosure, edit and destruction of the above data to authorized and legitimate personnel; protect the above data from accidental loss, destruction and compromise; prevent the above data from forseeable threats and compromise.

2. CFCA takes actions to verify the condifentiality, completeness and serviceability of the “Certificate data”, and the key, software and procedures used in certificate issuance, repository maintenance and certificate revocation.

3. CFCA ensures that the data it maintained are in line with the security demands of relevant laws and regulations.

6.5.2 Periodic Risk Assessment of Data Security

1. CFCA carries out periodic risk rating to identify the forseeable internal and external threats that may subject “Certificate data” and “Certificate procedures” to unauthorized acess, use, disclosure, edit and destruction;

2. According to the sensitivity of the “Certificate data” and “Certificate procedures”, the risk rating assesses the possiblitiy of the identified threats and the harm they are expected to cause.

3. Annual reviews are carried out on the controls to determine the comfort they bring, including the policies, procedures, information systems, technologies and other relevant factors.

6.5.3 Security Plan

Based on the above risk assessments, a security plan is made to address the making, implementing and maintaining security procedures and measures, and products designed for data security. Proper management and controls will be applied on identified risks according to the sensitivity of the “Certificate data” and “Certificate procedures”, as well as the complexitiy and scopes of the procedures.

The security plan should contain administrative and organizational structure, technical and physical controls adaptive to the scale, complexity, nature and scope

of the “Certificate data” and “Certificate procedures”. The design of security controls should consider available technologies in the future and corresponding costs. The controls should be aligned with the potential harm caused by the absence of the controls, and the nature of the data to be protected.

6.6 Computer Security Controls

According to the regulations on system security management, CFCA requires the CA and RA to use trustworthy and secure operation systems to provide services. The corporate clienst are required to do the same.

6.6.1 Specific Computer Security Technical Requirements

CFCA practices information security management that is in line with relevant national regulations. Key security technologies and controls include: secure and trustworthy operation systems, stringent identity authentication and access control policies, multi-layer firewall, segregation of duties, internal controls, and business continuity plans, etc.

6.6.2 Computer Security Rating

The CFCA Global Trust System has undergone the security appraisal of the State Cryptographic Administration and other relevant departments.

6.7 Life Cycle Technical Controls

6.7.1 Root Key Controls

The root key generation ceremony should be witnessed by a qualified auditor, who then issue a report opiniong that CFCA, during its root key and certificate generation process:

1) Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the “Root Key Generation Script”) for the Root CA;

2) Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script;

3) Performed, during the root key generation process, all the procedures required by its Root Key Generation Script;

4) A video of the entire key generation ceremony will be recorded for auditing purposes.

These stipulations are also applicable for the controls of other keys.

6.7.2 System Development Controls

The developers of CFCA’s systems meet relevant national security standards and possess manufacturing licenses of commercial cryptographic products. The development process also meets the requirements of the State Cryptographic

Administration.

6.7.3 Security Management Controls

CFCA follows the norms made by the competent department in practicing information security management of its systems. Any system change must udergo stringent tests and reviews before implementation and use. At the same time, CFCA has set up strong management policies based on the ISO9000 quality management system standards. Core data is backuped daily according to a scheduled timetable by dedicated personnel. Data recovery is performed monthly by dedicated personnel to test the serviceability of the data.

6.7.4 Life Cycle Security Controls

The developers of CFCA's systems meet relevant national security standards and possess manufacturing licenses of commercial cryptographic products. The development process also meets the requirements of the State Cryptographic Administration. The source code of the systems is backuped at the State Cryptography Administraion to ensure system continuity.

6.8 Network Security Controls

CFCA employs the following measures to protect its networks from unauthorized access and hostile attacks:

1. Screen external access information through the router;

2. Place servers with independent functions at different network segments;

3. Set up multi-layer firewall, spilt the network, and implement robust access control technologies;

4. Protect data through verification and access controls;

5. Install intruder detection products in the network to protect the network through inspection and monitoring, so that CFCA can be alerted of and respond to intruders as soon as possible;

6. All terminals should be installed with anti-virus software, which is updated regularly;

7. Adopt redundancy design.

6.9 Time-Stamping

Certificates, CRLs, OCSP, and electronic certification system logs shall contain time and date information. Such time information should be consistent with the national standard time.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The format of Certificates issued by CFCA conforms to the digital certificate standard GM/T 0015-2012 and contains the following fileds.Please refer to Appendix B for the fields contained in EV SSL certificates.

7.1.1 Version Number(s)

CFCA certificates are X.509 V3 certificates. This information is contained in the “Version” field of the certificates.

7.1.2 Certificate Extensions

Certificate extension is an extended sequence for one or more certificates, and is targeted for a specific type of certificates or specific users. The certificates issued by CFCA contain private extensions, which are set as non-critical extensions. The extensions of root CA certificate follow the RFC 5280 standard except four extensions: Basic Constraints, Key Usage, Certificate Policies and Extended Key Usage.

7.1.2.1 Authority Key Identifier

CFCA populates the Authority Key Identifier extension subscriber certificates and CA certificates. This extension is used to identify the corresponding public key of the private key that signed the certificate, and thus distinguish the different keys used by the same CA. It’s a non-critical extension.

7.1.2.2 Subject Key Identifier

The subscriber certificates are populated with the Subject Key Identifier, which marks the public key contained in the certificate, and is used to distinguish the different keys used by one subscriber (e.g.certificate rekey). Its value is

exported from the public key or by generating a unique value. This is a non-critical extension.

7.1.2.3 Key Usage

The Key Usage extension defines the usages of the public key contained in the certificate, including certificate signing and CRL issuing.It's a critical extension for CA certificates, and a non-critical extension for subscriber certificates.

7.1.2.4 Basic Constraints

Basic Constraints is used to label whether a certificate subject is a CA, and determine the possible certification path length.The extension follows the RFC3280 standards. It's a critical extension for CA certificates, and a non-critical extension for subscriber certificates.

7.1.2.5 Extended Key Usage

This extension is used to indicate the one or more uses that are supplements or substitutes of the uses stated in the Key Usage extension.

For SSL server certificates, EV SSL certificates, Device certificates, and VPN certificates, this field is serverAuth.

For code signing certificates, this field is codeSigning and timeStamping .

For individual and corporate certificates, this field is clientAuth.

For email certificates, the field is emailProtection.

7.1.2.6 CRL Distribution Points

Certificates include the CRL Distribution Points extension which can be used to locate and downlown a CRL. This extension MUST present and MUST NOT be marked Critical. (As in BR Appendix B)

7.1.2.7 Subject Alternative Names

The Subject Alternative Names extension contains one or more alternative names (can be in any name form) for the certificate subject. CA binds the subject with the public key contained in the certificate. The extension is populated in accordance with the RFC3280 and RFC 2459 standards.

SSL certificates, EV SSL certificates, email certifiates must contain this field. It is optional for other types of certificates.

All information contained in the filed must be verified by CFCA.

7.1.3 Algorithm Object Identifiers

The SSL certificates issued by CFCA are signed using SHA-256 RSA and SM2-SM3 algorithms, and comply with RFC 3280 standards.

The OID of SM2 algorithm is 1.2.840.10045.2.1, extra parameter is 1.2.156.10197.1.301.

7.1.4 Subject Name

This section describes the entity's situation corresponding to the subject field in the pulic key. CFCA follows the X.500 standards on distinguished name (DN). DN is used to describe the corresponding entity of the public key. CFCA makes sure that the DN is unique by establishing the CFCA Certificate DN Rule and The Pre-generated Certificate DN Rules.All information contained in the certificate is verified by the CFCA.

The following 5 parts must be included in the OCA 21 Certificate Issuance:

1、 CN: refer to CFCA Certificate DN Rule V5.1 and Pre-generated Certificate DN Rule V2.0 for details

2、 OU【2】: indicates certificate types as follows:

Types	OU
Individual Normal	Individual-1
Individual Advanced	Individual-2
Business Normal	Organizational-1
Business Advanced	Organizational-2

3、 OU【1】: Indicates the name of RA which can be in English or Pinyin.For example, the CITIC bank: OU=CITIC。In terms of pre-generated certificate, this indicates the system name that provides the service. For example, OU[1]=TPC-S1。

If any entity name or its abbreviation appears in OU, CFCA would verify accordingly.

4、 O: Indicates the name of CA.

5、 C: indicates the abbreviation of the country of the applicant, all in capital form. For example, Chinese subscriber would be indicated as C=CN

The DN of the certificates issued by the OCA2 system include the following 5 parts:

1、 CN: The real name of the Entity

2、 OU【2】: Optional. To indicate the department name of the entity or certificate types:

Types	OU
SSL Certificate	GTC
Code Sigining Certificate	Code Signing
Secure Email Certificate	Email
VPN Certificate	VPN
Device Certificate	Device

If OU indicates the department name of an entity, CFCA must verify this part.

3、 OU【1】: Optional. This could indicate the department name of an entity or the name of CFCA’s local RA.

For example, CFCA's local RA: OU=Local RA。

If OU indicates the department name of an entity, CFCA must verify this part.

4、 O: indicates the name of the entity. If English is used, the name must be consistent with the meaning of the name on the valid ID to avoid misunderstanding.

5、 C: indicates the abbreviation of the country of the applicant, all in capital form. For example, Chinese subscriber would be indicated as C=CN

DN may also contain attributes "E", "L" and "S". "E"is used to bind the email address of the subscriber with the certificate. The attribute "CN"should be put in the front of a DN. The other attributes would be arranged according to their value from the smallest to the largest. "O" would be placed before "OU", "L" before "S". The last must be "C".

The country, province and city names in the DN must be those listed in the standards released by authorities (e.g. ISO country code).

For Email Certificate, "E" is a must, while the real name of the subscriber must be put in the "CN" attribute. As to the certificates issued under OCA2, the subscriber must generate a Certificate Signature Request (CSR) before the certificate request. After it's verified by CFCA, it would be used in the certificate issuance.

Please refer to Appendix B for the DN field of certificates issued by EV OCA.

7.1.5 Name Constraints

Subscribers are not permitted to use anonymity or pseudonymity. The names must be distinguished names with clear meaning. When English names are used, they must be able to identify the entities.

7.1.6 Certificate Policy Object Identifier

When the Certificate Policies extension is used, the "certificatePolicies:policyIdentifier" field should be set to "anyPolicy".

Certificate Policy OIDs of subscriber certificates are as follow:

EV Certificate Policy OID = 2.16.156.112554.3. The Certificate Policy extension of EV certificate states that a certificate is marked as an EV certificate according to the Guidelines for the Issuance and Management of Extended Validation Certificates V1.4, as well as the convention with the application developer. The application developer stores the EV OID of the CA in the master record to identify the root CA that can be used to issue EV certificates.

GT OCA2 Certificate Policy OID = 2.16.156.112554.2.1

GT OCA21 Certificate Policy OID = 2.16.156.112554.2.2

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Not applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL

7.2.1 Version Number(s)

CFCA uses X.509 V2 CRL.

7.2.2 CRL and CRL Entry Extensions

CRLs conform to RFC 5280 and contain fields and contents specified below:

1. Version

The version of the CRL

2. Issuer

The distinguished name of the CA that issues the CRL.

3. This Update

Issue date of the CRL.

4. Next Update

Date by which the CRL will be issued.

5. Signature Algorithm

6. Revoke Certificates

Listing of revoked certificates, including the serial number of the revoked certificate and the revocation date.

7.Crl Number

This Number will increase after each update of CRL.

7.3 OCSP Profile

CFCA EV system provides Online Certificate Status Protocol services. The other systems provide this service according to business demand.

On a network working normally, CFCA ensures adequate resources to provide the result for an inquiry on CRL and OCSP within a reasonable span of time.

CFCA validates:

Certificates using CFCA OCSP Service conforms to RFC2560.

7.3.1 OCSP signer Certificates

OCSP signer Certificate share the same standard with End-Entity Certificates(Including Public key length and validity period). Conforms to Baseline Requirement and the related field in RFC5280.

~~7.3.1~~7.3.2 Version Number(s)

Version 1 of the OCSO specification as defined by RFC2560.

Formatted: Font: 16 pt

Formatted: Font: 14 pt

Formatted: Indent: First line: 2 ch

Formatted: Indent: First line: 0.29", Outlin numbered + Level: 3 + Numbering Style: 1, 3, … + Start at: 1 + Alignment: Left + Align at: 0.44" + Tab after: 0.74" + Indent at: 0.4

Formatted: Font: 14 pt

Formatted: Indent: First line: 2 ch

Formatted: Font: 10.5 pt

Formatted: Indent: First line: 0 ch

8 Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

Following are the assessment performed:

1、 Assessments and inspections by the competent department based on the Electronic Signature Law of the People's Republic of China, the Methods for the Administration of Electronic Certification Services, the Methods for the Administration of Cipher Codes for Electronic Certification Services.

2、 Regular assessments carried out by external accounting organizations.

3、 Webtrust and EV audits carried out by third party accounting firms.

Assessment frequency:

1、Annual assessment: the competent department carries out annual reviews on CFCA.

2、Pre-issuance assessment: Before launching a new system, it must be reviewed and signed off by the competent department.

3、Regular assessment: Regular assessments are carried out by external auditors according to relevant international or domestic standards and requirements.

4、Annual Webtrust and EV assessments are carried out with the reports released within three months after period end.

8.2 Identity/Qualifications of Assessor

Compliance audits are performed on CFCA by an experience accounting firm that demonstrates profiency in IT operation management, public key infrastructure technology, relevant laws, regulations and standards.

The external auditors should:

Be with an independent accounting firm that is qualified to provide third party certification on information science and technology, information security, PKI and system audit;

Hold valid qualifications on EV certificate Webtrust and Webtrust assurance when the services are provided;

Be the members of AICPA or other association with clear qualification standards for its members.

8.3 Assessor's Relationship to Assessed Entity

The assessor should have no business relationship, financial interest or any other interest relation with CFCA.

8.4 Topics Covered by Assessment

Assessment topics should include but are not limited to the following:

1. Physical environment and controls
2. Key management operations
3. Basic controls

4. Certificate life cycle management

5. Certificate Practice Statement

8.5 Actions Taken as a Result of Deficiency

CFCA management should review the audit reports and take corrective actions on significant exceptions and omissions identified in the audits within 20 days after audit completion.

8.6 Communications of Results

The competent department will release the assessment results on CFCA after their inspections and reviews.

CFCA will release the results of external audits on its website.

Results of internal audits are communicated inside CFCA.

8.7 Other Assessment

CFCA controls the service quality through continual self-assessments, on a quarterly basis. Compliance to relevant policies and rules are assessed during the assessment period. During the period in which it issues Certificates, CFCA will control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the Certificates it has issued in the period beginning immediately after the last sample was taken. For EV certificates, compliance to EV certificates standard would be examined, and the sample

selected would not be less than 3% of the certificates issued in the period.

9 . Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

At the point of certificate purchase, CFCA informs the subscribers of the fees for certificate issuance and renewal, charged according to the regulations of the marketing and management departments.

9.1.2 Certificate Access Fees

CFCA does not charge a fee for this service, but reserves the right to do so.

9.1.3 Revocation or Status Information Access Fees

CFCA does not charge a fee for this service, but reserves the right to do so.

9.1.4 Fees for Other Services

CFCA reserves the right to charge a fee on the other services it provides.

9.1.5 Refund Policy

A refund shall no be provided unless CFCA has breached the responsibilities and obligations under this CPS.

CFCA shall not be held responsible for loss or consequence caused by the incomplete, unauthentic or inaccurate certificate request information submitted by the subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CFCA determines its insurance policies according to its business development and the business of domestic insurance companies. As for EV certificates, CFCA has undergone financial auditing provided by third party auditors, and has reserved insured amount for planned customers.

9.2.2 Other Assets

CFCA shall have sufficient financial resources to maintain its operation and perform their duties, and must be reasonably able to bear the responsibilities to subscribers and relying parties.

This clause is applicable for the subscribers.

9.2.3 Insurance or Warranty Coverage for End Entities

If according to this CPS or other laws and regulations, or judged by the judicial authorities, CFCA shall bear compensation and reimbursement obligations, CFCA would make compensation and reimbursement according to relevant laws and regulations, the ruling of the arbitral bodies and court decisions.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Information that shall be kept confidential and private includes but is not limited to the following:

1. Information contained in the agreements signed between CFCA and the subscribers, and relevant materials, which has not been publicized. Unless demanded by laws, regulations, governments and law enforcement agencies, CFCA shall not publicized or reveal any confidential information other than the certificate information.
2. Private keys held by the subscribers. The subscribers are responsible to custody the private keys according to the stipulations in this CPS. CFCA will not be held responsible for the private key leakage caused by the subscribers.

9.3.2 Information Not Within the Scope of Confidential Information

Following is information not considered confidential:

1. Information on the certificates issued by the CFCA, and on the CRL.
2. Data and information known by the receiving party piror to their release by the supplying party.

3. Information that becomes publicly known through no wrongful act of the receiving party, upon or after the supplying party reveals the data or information.
4. Data and information that are publicly known.
5. Data and information released to the receiving party by rightful third party.
6. Other information that can be obtained from open and public channels.

9.3.3 Responsibility to Protect Confidential Information

Stringent management policies, procedures and technical instruments have been employed by CFCA to protect confidential information, including but is not limited to business confidential information and client information. No employee of CFCA has not been trained on handling confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

CFCA respects all the subscribers and their privacy. The privacy plan is in conformity with valid laws and regulations. The acceptance of certification service indicates the subscribers' acceptance of the privacy plan.

9.4.2 Information Treated as Private

CFCA treats all information about subscribers that is not publicly available in

the content of a certificate, and certificate status information as private. The information are used only by CFCA. Private information shall not be revealed without the consent of the subscribers, or demands of judicial or public authorities raised pursuant to legitimate procedures.

9.4.3 Information Not Deemed Private

Content on the certificates and certificate status information are not deemed private.

9.4.4 Responsibility to Protect Private Information

CFCA, RAs, subscribers, relying parties and other organizations and individuals are obliged to protect private information according to the stipulations in this CPS. CFCA is entitled to disclose private information to specific parties in response to the demands raised by judicial and public authorities pursuant to legitimate procedures, and shall not be held responsible for the disclosure.

9.4.5 Notice and Consent to Use Private Information

1、 The subscribers consent that CFCA is entitled to use all information within its business practices according to the privacy policies stipulated in this CPS, and is not obliged to inform the subscribers.

2、 The subscribers consent that, CFCA may disclose private information when demanded to do so by judicial and public authorities, and is not

obliged to inform the subscribers.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Other than in the following occasions, CFCA shall not disclose confidential information to any other individual or third party organization:

1、 Legitimate applications have been proposed by judicial, administrative departments, and other departments authorized by laws and regulations, according to laws, regulations, decisions, orders and etc.

2、 Written warrants have been provided by the subscribers.

3、 Other occasions stipulated in this CPS.

9.4.7 Other Information Disclosure Circumstances

CFCA, subscribers, CA and other organizations and individuals are obliged to protect private information according to the stipulations in this CPS. CFCA is entitled to disclose private information to specific parties in response to the demands raised by judicial and public authorities pursuant to legitimate procedures, or when written warrants have been provided by the subscribers, and shall not be held responsible for the disclosure.

9.5 Intellectual Property rights

CFCA owns and retains all intellectual property rights, including the

copyrights and patent application rights on the certificates, software and data it provides. The CPS, CP, technical support manual, certificates and CRL are the exclusive properties of CFCA, who owns their intellectual property rights.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CFCA provides certification services using information security infrasture approved by relevant administrative authorities.

CFCA's operation is in conformity with the Electronic Signature Law of the People's Republic of China and other laws and regulations. It accepts the governance of the competent department. CFCA is legally responsible for the certificates it issues.

CFCA's operation is in conformity with this CPS, which is amended as the business changes.

According to the requirements of the Managing Rules for Electronic Certification, CFCA is responsible for auditing the delegated parties' compliance with the CPS and relevant requirements on an annual basis. CFCA retains the rights and responsibilities to keep and use subscribers' information.

9.6.2 RA Representations and Warranties

As registration authority of CFCA, It's responsible for verifying the identity of

the applicants, determining whether to accept or reject the certificate requests, inputting subscriber information into the RA systems, and deliver the requests infomation to the CA systems vir secure channel.

As the RA, CFCA represents and warrants that:

1、 It obides by its strategies and administrative regulations, verifies the certificate request materials for the completeness and accuracy of the information they contain. It's entitled to accept or reject the certificate requests.

2、 When RAs issue pre-generated certificates, the information contained in the certificates should be bound to the entity. The signature information should be securely delivered to CFCA, and the certificate can be activated for use after the RA receives the conformation from CFCA. Subscribers should be notified of the change of the default password of the intelligent password key and not to use the key in public place.

3、 RAs should design an appropriate business process that the pre-generated certificates are kept properly before issuing to the subscriber and that the certificate will not be used before it is bound to an entity.

4、 If CFCA rejects a certificate request, it's obliged to inform the corresponding subscriber. If CFCA accepts a certificate request, it's obliged to inform the corresponding subscriber, and assist the subscriber in obtaining the certificate.

5、 Certificate requests are handled in an reasonable period of time. Requests are handled within 1-3 working days provided the application materials

are complete and meet the requirements.

6、 RAs properly retains the information about the subscribers and the certificates and transfers the documents to CFCA for archival. RAs should cooperate with CFCA according to relevant agreements for compliance audit.

7、 RAs should make subscribers aware of the meaning, function, scope and method of using the third-party digital certificates as well as key management, result and response measures for key compromise, and legal responsibilities.

8、 CFCA informs the subscribers to read its CPS and other regulations. A certificate will only be issued to a subscriber who fully understand and consent the stipulations of the CPS.

9.6.3 Subscriber Representations and Warranties

Subscribers represent and warrant that:

They have read and understood the entire CPS and relevant regulations, and consented to be bound by this CPS.

They honor the principles of honesty and credibility; that accurate, complete and authentic information and materials are submitted in certificate application; that CFCA will be informed timely of any change in these information and materials.Loss caused by unauthentic information submitted intentionally or accidentially, or failure of the subscribers to inform CFCA when the information changes are borne by the subscribers.

They use the key pairs in trustworthy systems to prevent the keys from being

attacked, leaked or misused. They properly protect the private keys and passwords of the certificates issued by CFCA, and do not trust the other parties with the keys. If, accidentally or intentionally, the private keys or passwords are known, stolen or falsely used by others, the subscribers bear the corresponding responsibilities.

The subscribers or legal representatives request for certificate revocation at the original RA as soon as possible, and observe the procedures described in this CPS, if the private keys or passwords of the certificates have been leaked or loss, or the subscribers wish to terminate the usage of the certificates, or the subjects stop to exist,

The subscribers use the certificates in functions that are legitimate and consistent with this CPS.

The subscribers bear the responsibilities for using the certificates.

Subscribers will indemnify CFCA for:

1) Falsehood/incompleteness/misrepresentation of facts by the subscribers on the certificate application. Failure to give timely notice to CFCA when the facts change.

2) Failure to inform all relevant parties and revoke the certificates when the private keys are known to be or may have been lost.

3) Other wrongful acts or failure to honor the agreements.

Subscribers are obliged to pay certification service fee timely. Please consult the Marketing Department for charge standards.

CFCA is entitled to inform the subscribers to change their certificates as the

technologies progress. Subscribers shall submit certificate rekey request witin specified periods when they receive the notices. CFCA is not liable if the subscribers do not change their certificates timely.

9.6.4 Relying Party Representations and Warranties

Relying parties represent and warrant that:

1. They obtain and install the certificate chains corresponding to the certificates;

2. They verify that the certificates are valid before any act of reliance. To do so, relying parties need to obtain the latest CRL released by the CFCA to ensure that the certificates have not been revoked. All the certificates appear in the certificate pathes should be assessed on their reliability. Validity period of the certificates shall be checked. Relying parties shall also review other information that may affect the validity of the certificates.

3. They make sure that the content on the certificates is consistent with the content to be proved.

4. They obtain sufficient knowledge of this CPS and the usage of certificates, and use the certificates within the scope stipulated by this CPS.

5. They accept the limitation of CFCA's liability described in this CPS.

9.6.5 Representations and Warranties of Other Participants

The unidentified participants should observe the stipulations in this CPS.

9.7 Disclaimers of Warranties

1. CFCA is not liable for a dispute occur in the usage of the certificate, if the corresponding subscriber has intentionally not, or failed to provide accurate/authentic/complete information on the certificate application.

2. CFCA is not liable for loss caused by certificate failure, transaction interruption or other incidents, which are caused by device and network breakdown that has happened through no wrongful act of CFCA.

3. CFCA is not liable if the certificate has been used in functions not intended or prohibited by CFCA.

4. CFCA is not liable if parts of or all of the certification services of CFCA have been suspended or terminated becaused of force majeure.

5. CFCA is not liable for using services other than CFCA's service of digital signature verification in online transactions.

6. CFCA is not liable for the breach of agreement caused by a patner's ultra vires behavior or other mistakes.

9.8 Limitations of Liability

If according to this CPS or other laws and regulations, or judged by the judicial authorities, CFCA shall bear compensation and reimbursement obligations, CFCA would make compensation and reimbursement according to relevant laws and regulations, the ruling of the arbitral bodies and court decisions.

9.9 Indemnities

9.9.1 Unless otherwise stipulated or agreed, CFCA is not liable for any loss not caused by the certification service stated in this CPS.

9.9.2 CFCA shall compensate, according to this CPS, the subscriber or relying party, who suffers loss caused by the certification service provided by CFCA. However, CFCA shall not be deemed faultful if it can prove that it has provided services according to the Electronic Signature Law of the People's Republic of China, the Methods for the Administration of Electronic Certification Services and the CPS filed to the competent department, and shall not be required to bear any compensation and reimbursement responsibility towards the subscriber or relying party.

9.9.3 CFCA is not liable for the following, whether it has infringed this CPS or not:

(1) Any indirect loss, direct or indirect loss of profit or income, compromise of reputation or goodwill, loss of business opportunities or chances, loss of projects, loss or failure to use data, device or software;

(2) Any loss or damage caused directly or indirectly by the above loss.

9.9.4 If according to this CPS or other laws and regulations, or judged by the judicial authorities, CFCA shall bear compensation and reimbursement obligations, CFCA would make compensation and reimbursement according to relevant laws and regulations, the ruling of the arbitral bodies and court decisions.This is so whether or not this CPS contains contradictive or

different regulations.

9.10 Term and Termination

9. 10. 1 **Term**

This CPS becomes effective upon publication on CFCA's official website (http://www.cfca.com.cn). Unless otherwise announced by CFCA, the previous CPS is terminated.

9. 10. 2 **Termination**

CFCA is entitled to terminate this CPS (including the revisions). This CPS (including the revisions) shall be terminated upon the 30th day after CFCA posts a termination statement on its official website.

The CPS shall remain in force until a new version is posted on CFCA's official website.

9. 10. 3 **Effect of Termination and Survival**

Upon termination of this CPS, its provisions on auditing, confidential information, privacy protection, intellectual property rights, and the limitation of liability remain valid.

9.11 Individual Notices and Communications with Participants

To learn more about the service, norms and operations mentioned in this CPS, please contact CFCA at 010-83526220.

9.12 Amendments

CFCA is entitled to amend this CPS and will release the revised version on its official website.

9.12.1 Procedure for Amendment

The procedure for amendment is the same as Section 1.5.4 “CPS Approval Procedure”.

9.12.2 Notification Mechanism and Period

CFCA reserves the right to amend any term and provision contained in this CPS without notice. But the revised CPS will be posted on the CFCA website in a timely manner. If the subscriber doesn’t request for certificate revocation within seven days after the publication, it will be deemed to have accept the amendment.

9.12.3 Circumstances under Which CPS Must be Amended

CFCA shall amend this CPS if: the rules, procedures and relevant technologies stated in this CPS can no longer meet the demands of CFCA’s

certification business; the governing laws and regulations of this CPS have changed.

9.13 Dispute Resolution Provisions

If a subscriber or relying party discover or suspect that leakage/tampering of online transaction information has been caused by the certification service of CFCA, it shall submit a dispute resolution request to CFCA and notice all related parties within three months.

Dispute resolution procedures:

1. Notice of dispute

When a dispute occurs, the subscriber should notice CFCA before any corrective action is taken.

2. Resolution of dispute

If the dispute is not resolved within ten days following the initial notice, CFCA will set up an external panel of three external certificate experts. The panel will collect relevant facts to assist the resolution of the dispute. Panel opinion should be formed within ten days following the foundation of the panel (unless the parties concerned agree to extend this period) and delivered to the parties. Panel opinion is not binding on the parties concerned. The signing of the panel opinion by the subscriber of relying party constitutes acceptance of the opinion. As a result, the dispute will be solved according to the panel opinion. The panel opinion will then be reviewed as the agreement between CFCA and the subscriber on the resolution of the dispute and is legally binding. Thus, if the subscriber wants to pull out of the agreement, and submit the dispute to arbitration, it will be bound by the panel opinion to do so.

3. Formal Resolution of Dispute

If the panel fails to put forward effective opinion in the time agreed upon, or the opinion doesn't enable the two parties to agree on the resolution, the parties shall submit the dispute to the Beijing Arbitration Commission.

4. Time Limit for Claim

If the subscriber or relying party plans to make a claim on CFCA, it shall do so within two years after it becomes aware or should be aware of the loss. After this period, the claim is invalid.

9.14 Governing Law

Governing laws of the CFCA CPS include the Contract Law of the People's Republic of China, the Electronic Signature Law of the People's Republic of China and other relevant laws and regulations. If any clause in this CPS is in conflict with the above laws and regulation, or is unenforceable, CFCA shall amend the clause in question till this situation is resolved.

9.15 Compliance with Applicable Law

All the policies of CFCA are in compliance with applicable laws, regulations and requirements of the People's Republic of China and the state information security authorties. In the event that a clause or provision of this CPS is held to be illegal, unenforceable or invalid by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid. CFCA will amend that clause or provision until it's legitimate and enforceable.

9.16 Miscellaneous Provisions

9. 16. 1 Entire Agreement

The CPS renders invalid the written or verbal explanations on the same topics during the previous or same periods. The CPS, CP, Subscriber Agreement, Relying Party Agreement and their supplement agreements constitute the Entire Agreement for all participants.

9. 16. 2 Assignment

The CA, subscribers and relying parties are not allowed to assign their rights or obligations in any form.

9. 16. 3 Severability

In the event that a clause or provision of this CPS is held to be illegal, unenforceable or invalid by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid. CFCA will amend that clause or provision until it’s legitimate and enforceable.

9. 16. 4 Enforcement

Not applicable.

9.16.5 Force Majeure

Force majeure refers to an objective situation that is unforeseeable, unavoidable and irresistible. Examples of force majeure include: war, terrorist attack, strike, natural disaster, contagious disease, and malfunction of internet or other infrastructure. But all pariticipants are obliged to set up disaster recovery and business continuity plan.

9.17 Other Provisions

CFCA warrants observing the latest verion of Guidelines for the Issuance and Management of Extended Validation Certificates released by the CA/Browser Forum and the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificatess (From http://www.cabforum.org.). Should there be any inconsistency between the CPS and the above Guidelines, the latter shall prevail.

Appendix Definitions and Acronyms

Table of Acronyms

Term	Definition
ANSI	（The American National Standards Institute）
CA	（Certificate Authority）
RA	(Registration Authority)
CRL	(Certificate Revocation List)

OCSP	(Online Certificate Status Protocal)
CP	(Certificate Policy）
CPS	（Certificate Practice Statement）
CSR	（Certificate Signature Request）
IETF	(The Internet Engineering Task Force)

Definitions

Term	**Definition**
Certificate Authority	An authority trusted by the subscribers to generate, issue and manage public keys and certificates; and generate private keys for the subscribers in some occasions.
Registration Authority	An entity responsible for handling the application, approval and management of certificates.
Certificate	An electronic file that contains the indentity and public key of the Subscriber, and is digitally signed by the CA.
Certificate Revocation List	A list issued periodically under stringent requirement, digitally signed by the CA, and indicates the certificates that are no longer trusted by the CA.
Online Certificate Status Protocal	A protocol issued by IETF providing information of certificate status.
Certificate Policy	A certificate policy (CP) is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate the applicability of a type of certificate for the B-to-B trading of goods or services within a given price range.
Certification Practice Statement	A certification practice statement is a statement of practices that the CA employs in certificate issuance, management, revocation and renewal (or renewing the private key of the certificate).
Subscriber	。 An entity applying for the certificate.
Relying Party	A relying party is an individual or organization that acts on reliance of the trust relations proved by the certificate.
Private Key	An encryption key generated through arithmetical operation (kept by the holder) to create digital signature, and/or to decrypt electronic records or files that were encrypted with the corresponding public key (to ensure information confidenetiality).
Public Key	An encryption key generated through arithmetical operation made public by the holder, and that is used to verify the digital signature created with the corresponding private key, and/or to encrypt messages or files so that they can be decrypted only with the holder’s corresponding private key.
Distinguished Name	A distinguished name is contained in the Subject name field on the certificate and is

	the unique indentifier of the subject. The distinguished name should follow the X.500 standard, reflect the authentic identity of the subject, is of practical meaning, and in conformity with laws.

Appendix B

Format of EV SSL Certificate		
Field	**Value**	
Version	V3	
Serial Number	Contains 20 non-serial digits	
Algorithm	SHA256RSA	SM2/SM3（1.2.156.10197.1.501）
Issuer	CN = CFCA EV OCA O = China Financial Certification Authority C = CN	CN = CFCA EV SM2 OCA O = China Financial Certification Authority C = CN
Valid from		Certificate Valid from
Valid to		Certificate Expiry date
Subject	CN = pub.cebnet.com.cn	Compulsory and contains only domain name
	OU = E-banking network	Name of the department
	O = China E-banking network	Legal organisation name. If unofficial name is used, it should correctly reflect the organisation name and no misleading interpretation are caused. If the name exceeds 64 bytes, abbreviation should be used, but no misleading interpretation should be caused.
	L = Beijing	Business Address: including Country, State or Province, City or Village, Street, Postcode. Country, State or Province,City or village are compulsory, and street and postcode are optional.
	S = Beijing	
	SERIALNUMBER = 110000006499259	ID number (eg. Orgniasation code,

		Business certificate code, tax registration code). Or date of establishment if no registered ID number provided.
	2.5.4.15 = Private Organization	Business Type: one of the following Private Organization Government Entity Business Entity Non-Commercial Entity
	1.3.6.1.4.1.311.60.2.1.1 = Registered Area	Registered address
	1.3.6.1.4.1.311.60.2.1.2 = Registered Province	
	1.3.6.1.4.1.311.60.2.1.3 = CN Country code of registered country	
Public Key	RSA (2048)	1.2.840.10045.2.1 (SM2 Algorithm identifier)
Authority Information Access	[1]Authority Info Access Access Method=on-line certificate protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method=Certificate Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://gtc.cfca.com.cn/evoca/evoca.cer	
Authority Key Identifier		
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.156.112554.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-12.htm	2.16.156.112554.3 is the identifier of EV SSL certificate issued by CFCAhttp://www.cfca.com.cn/us/us-12.htm is the EV Certificate Policy address
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cfca.com.cn/evoca/RSA/crl1.crl	CRL distribution point of EV SSL Certificate
Key Usage	Digital Signature, Key Encipherment (a0)	
Subject Key Identifier		

Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)	

Appendix C

Format of SSL Certificates		
Field	**Value**	
Version	V3	
Serial Number	Contains 20 non-serial digits	
Algorithm	SHA1RSA	SM2/SM3（1.2.156.10197.1.501）
Issuer	CN = CFCA OCA2 O = China Financial Certification Authority C = CN	CN = CFCA SM2 OCA2 O = China Financial Certification Authority C = CN
Valid From		Certificate Valid Starting Date
Valid To		Certificate Expiry Date
Subject	CN = pub.cebnet.com.cn	Compulsory and must be domain name or external IP address
	OU = E-banking network	Department name or certificate type（non compulsory）
	OU=LOCAL RA	Department name or RA name（non compulsory）
	O = China E-banking network	Legal organisation name. If unofficial name is used, it should correctly reflect the organisation name and no misleading interpretation are caused. If the name exceeds 64 bytes, abbreviation should be used, but no misleading interpretation should be caused.
	L = Beijing	Business Address: including Country, State or Province, City or Village, Street, Postcode. Country, State or Province, City or village are compulsory, and street and postcode are optional.
	S = Beijing	
	C=CN	Country Code
Public Key	RSA（2048）	1.2.840.10045.2.1（SM2 Algorithm identifier）
Authority Information Access	[1]Authority Info Access Access Method= on-line certificate protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.cfca.com.cn/ocsp [2]Authority Info Access Access Method= Certificate Authority	

	Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://gtc.cfca.com.cn/gtoca/gtoca2.cer	
Authority Key Identifier		
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.156.112554.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-11.htm	2.16.156.112554.2.1 is the SSL identifier of certificates issued by CFCA http://www.cfca.com.cn/us/us-11.htm is the address of SSL certificate policies
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.cfca.com.cn/gtoca/RSA/crl1.crl	CRL distribution point
Key Usage	Digital Signature, Key Encipherment (a0)	
Subject Key Identifier		
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) S (1.3.6.1.5.5.7.3.1)	

Appendix E

Data Source Accuracy(comply with Baseline Requirement)

Prior to using any data source as a Reliable Data Source, the CFCA will evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CFCA will consider the following during its evaluation:

1. The age of the information provided;

2. The frequency of updates to the information source;

3. The data provider and purpose of the data collection;

4. The public accessibility of the data availability;

5. The relative difficulty in falsifying or altering the data.

(D) basicConstraints

This extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The cA field MUST be set true. The pathLenConstraint field MAY be present.

(E) keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. All other bit positions MUST NOT be set.

All other fields and extensions SHALL be set in accordance to RFC 5280.

(3) Subscriber Certificate

(A) certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for the CA"s extended validation policy.

certificatePolicies:policyIdentifier (Required)

EV policy identifier

certificatePolicies:policyQualifiers:policyQualifierId (Required)

id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri (Required)

HTTP URL for the Subordinate CA's Certification Practice Statement

(B) cRLDistributionPoint

This extension SHOULD be present and MUST NOT be marked critical. If present, it MUST contain the HTTP URL of the CA"s CRL service. This extension MUST be present if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension. See Section 11 for details.

(C) authorityInformationAccess

This extension SHOULD be present and MUST NOT be marked critical. If present, it MUST contain the HTTP URL of the CA"s OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1).

An HTTP URL MAY be included for the Subordinate CA"s certificate (accessMethod =

This extension MUST be present if the certificate does not contain a cRLDistributionPoint extension. See Section 11 for details.

(D) basicConstraints (optional)

If present, the cA field MUST be set false.

(E) keyUsage (optional)

If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

(F) extKeyUsage

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

All other fields and extensions SHALL be set in accordance to RFC 5280.