CFCA Certificate Policy and Certification Practice Statement for Global Trusted System

（CFCA Global-Trust CP&CPS）

V4.4

November 2022

History of Changes

Ver.	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 latest 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
3.0	Amend	Amend related content, add OV CodeSign, OV SSL Certificate,EV codesign related sections	Zhao Gaixia; Zhang Yi	Security Committee	Aug 2015
3.1	Amend	Amend related content, Amend OV CodeSign, OV SSL Certificate,EV codesign related sections	Zhang Yi	Security Committee	June 2015
3.2	Amend	Related section amended according minutes on Security Committee on June 24th， 2016	Zhao Yexin	Security Committee	June 2016

3.3	**Amend**	**Delete CFCA GT CA and OCA2\OCA21 contents. Since January 1st 2016, CFCA GT OCA2 stopped to issue new certificates and business would be substituted by CFCA OV OCA and practice statements of CFCA GT OCA21 would be described in CFCA CPS; Add CAA check action（effextive since September 1st，2017）. Version information revised.**	**Sun Shengnan**	**Security Committee**	**September 2017**
4.0	**Amend**	**Delete EV CodeSign certificates, OV CodeSign certificates contents; Add CT contents; Amend document structu, amend certificates verify data and methods according to CA/B requirements**	**Sun Shengnan**	**Security Committee**	**June 2019**
4.1	**Amend**	**Revise the division of work according to department adjustment; Delete CFCA EV SM2 OCA and CFCA OV SM2 OCA content;Add CFCA Global ECC ROOT CA1，CFCA Global RSA ROOT CA1，CFCA EV ECC OCA1，CFCA OV ECC OCA1，CFCA EV OCA1，CFCA OV OCA1 content; Text correction**	**Bi Xinlong**	**Security Committee**	**July 2020**
4.2	**Amend**	**Update Mozilla Root store Police, BR and EV Guidelines compliance**	**Bi Xinlong**	**Security Committee**	**July 2021**

		descriptions, update content according to the RFC 3647；add DV SSL Certificate content； Text correction			
4.3	**Amend**	**According to BR, update identification and authentication, revise name uniqueness description, supplement data source accuracy and CAA; adjust certificate revocation content; add description that certificate no longer contains OU**	**Qiu Dawei**		**July 2022**
4.4	**Amend**	**Update the document to " Certificate Policy and Certification Practice Statement Of CFCA Global-Trust System"; Adjusted CP&CPS update frequency; Adjusted the position of CAA chapters**	**Qiu Dawei**		**November 2022**

Table of Contents

1 Introduction

1.1 Overview

Established on June 29th, 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 Certificate Policy (CP) is a set of policies formulated by certification authority (CA), which indicates the division and obligations of each participant in the CFCA PKI system, and includes the basic policy of CFCA certificates.

A Certification Practice Statement (CPS) is a detailed description and statement of the practices which a certification authority (CA) follows in the whole life cycle of digital certificates (i.e. certificates) (e.g. issuance, revocation, and renew). It also describes the details of the business, technologies and legal responsibilities.

This CP&CPS is the certificate policy and certification practice statement for CFCA Global Trusted System. The Appendix D shows the system structure.

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

a) Due to SHA1 Deprecation Policy, CFCA decide to stop issuing SHA1 Certificate within Global Trust System since Jan 1st 2016, for those already have SHA1 certificate and it's valid date is after Jan 1st，2017, CFCA will assist subscriber upgrade to SHA256.

b) Due to CFCA business adjustment, CFCA stopped the issuance and renew of OV CodeSign certificates and EV CodeSign Certificates. The subordinate CAs, i.e. CFCA EV CodeSing OCA and CFCA OV CodeSign had been revoked on October 26th, 2018.

This CP&CPS conforms to Electronic Signature Law of the People's Republic of China; Cryptography Administration of Electronic Certification Services by OSCCA; Methods for the Administration of Electronic Certification Services and Specification of Electronic Certification Practices (Trial Version) by MIIT; the latest versions of GB/T 25056 Specification of Cryptography and Related Security Technology for Certificate Authentication System RFC 3647, Web Trust, Guidelines For The Issuance And Management Of Extended Validation Certificates, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates by CA/B Forum and other common practices of CA.

CFCA meets the requirements of WebTrust and has been audited by external auditors. CFCA holds valid License of Electronic Certification Services issued by MIIT and valid License of Crypytography Use in Electronic Certification Services.

1.2 Document Name and Indentification

This document is the Certificate Policy and Certification Practice Statement of CFCA Global-Trust System (CFCA Global-Trust CP&CPS).

CFCA has registered the corresponding Object Identity (OID) of this document in the National Registraion Center for OID. The OID included in this document iare：

No	Type of OID	OID	Description
1	Document Identifier	2.16.156.112554.2	CFCA Global Trust System CP&CPS
2	Certificate Identifier	2.16.156.112554.2.1	SSL Cert by OCA2
3	Certificate Identifier	2.16.156.112554.3	EV SSL Cert
4	Certificate Identifier	2.23.140.1.1	EV SSL Cert (required by Baseline Requirements)
5	Certificate Identifier	2.16.156.112554.4.1	OV SSL Cert
6	Certificate Identifier	2.23.140.1.2.2	OV SSL Cert (required by Baseline Requirements)
7	Certificate Identifier	2.16.156.112554.4.3	DV SSL Cert
8	Certificate Identifier	2.23.140.1.2.1	DV SSL Cert (required by Baseline Requirements)
9	Extension Field Identifier	1.3.6.1.4.1.11129.2.4.2	Certificate Transparency (require by main Root CA

			programs)

1.3 PKI Participants

PKI participants appear in this document includes Certification Authorities, Registration Authorities, Relying Parties and other participants. Followings are the descriptions.

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. It refers to CFCA only in this CP&CPS.

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 CFCA EV OCA, CFCA OV OCA, CFCA DV OCA, CFCA EV ECC OCA, CFCA OV ECC OCA, CFCA DV ECC OCA, CFCA EV RSA OCA, CFCA OV RSA OCA, CFCA DV RSA OCA under the CFCA Global Trust System is performed by CFCA internally and never entrust other facilities with this function.

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 CP&CPS to distinguish between two different roles: "Subscriber", is the entity，individual or organization generally, which contracts with CFCA for the issuance of certificates; “Subject", is the entity which the certificate is bound to. The “Subject” of SSL 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 trust party that is authenticated to which the certificate presents.

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.

1.4 Certificate Usage

1. 4. 1 Appropriate Certificare Uses

CA	Server
CFCA EV OCA	EV SSL Certificate(RSA)
CFCA OV OCA	OV SSL Certificate(RSA)
CFCA DV OCA	DV SSL Certificare(RSA)
CFCA EV ECC OCA	EV SSL Certificate(ECC)
CFCA OV ECC OCA	OV SSL Certificate(ECC)
CFCA DV ECC OCA	DV SSL Certificate(ECC)
CFCA EV RSA OCA	EV SSL Certificate(RSA)
CFCA OV RSA OCA	OV SSL Certificate(RSA)
CFCA DV RSA OCA	DV SSL Certificate(RSA)

CFCA EV ROOT, CFCA Global ECC ROOT and CFCA Global RSA ROOT are only used for signing subordinate CA certificates

1.4.1.1 CFCA EV SSL Certificate

CFCA EV SSL Certificate includes Multi-Domain Certificate and Singal Domain Certificate. EV SSL Certificates can be used to create a safe tunnel between the browser and the web server for encrypted transmission of data and prevent information leakage.

CFCA EV SSL Certificates are issued by CFCA EV OCA, CFCA EV RSA

OCA and CFCA EV ECC OCA. Their key sizes are RSA-2048 or ECC-256.

1.4.1.2 CFCA OV SSL Global Server Certificate

CFCA OV SSL Certificate includes Wildcard Certificate/ Multi-Domain Certificate/ Single Domain Certificate. OV SSL Certificates can be used to create a safe tunnel between the browser and the web server for encrypted transmission of data, and prevent information leakage.

CFCA OV SSL Certificates are issued by CFCA OV OCA, CFCA OV RSA OCA and CFCA OV ECC OCA. Their key sizes are RSA-2048 or ECC-256.

1.4.1.3 CFCA DV SSL Certificate

CFCA DV SSL Certificate includes Wildcard Certificate/ Multi-Domain Certificate/ Single Domain Certificate. DV SSL Certificates can be used to create a safe tunnel between the browser and the web server for encrypted transmission of data, and prevent information leakage.

CFCA DV SSL Certificates are issued by CFCA DV OCA, CFCA DV RSA OCA and CFCA DV ECC OCA. Their key sizes are RSA-2048 or ECC-256.

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 Strategic Development Department of CFCA. It sets up the "CP&CPS Team" to compile or amend this CP&CPS when needed. The General Manager can also set up a temporary CFCA team and appoint a person to take charge of the drafting or revision.

1.5.2 Contact

Any question on this CP&CPS, please contact the Strategic Development Department:

Tel: 010-80864996	Fax: 010-63555032
E-Mail: cps@cfca.com.cn	Address: NO.20-3, Pingyuanli, Caishikou South

	Avenue, Xicheng District, Beijing, P.R. China

1.5.3 Organization Dertermining CP&CPS Suitability for the Policy

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

1.5.4 CP&CPS Approval Procedures

The CP&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 CP&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 Strategic Development Department, who determines the format and version number of the CP&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

CP&CPS is posted on CFCA website. Paper CP&CPS is delivered to the clients and partners. The Strategic Development Department coordinates related parties in the publication.

The online publication of the CP&CPS follows the *CFCA Website Management Methods*. CP&CPS publicized in other forms should be consistent with the one posted on the website. The Strategic Development Department will report the CP&CPS to the competent department within 20 days following the publication.

The content of CP&CPS is regularly reviewed by the Strategic Development Department to initiate revision applications. The other departments can also raise a revision request depending on the demands of business. The CP&CPS can also be modified according to the relevant standards that the CP&CPS complies to.

This CP&CPS is updated at least once every year. If pervasive revision is needed, CFCA will adopt the same procedures of making the first version. If minor revision is needed, the Risk & Compliance Deparment will revise the CP&CPS and submit it to the leaders and managers to review. The CP&CPS, once approved by the General Manager, will be released on the corporate website. Every revised CP&CPS will be reported by the Strategic Development Department within 20 days following the publication.

1.6 Definitions and Acronyms

Please refer to Appendix A 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, CP&CPS, Certificate Service Agreement, technical support manual, CFCA website information and aperiodicity information released by CFCA.

2.2 Publication of Certification Information

CFCA releases CP&CPS and techinal support information on its website. Certificates defined in this CP&CPS will publish certificate log in extension field “Certificate Transparency” (SCT List) to satisfy main Root CA program requirements.

2.3 Time or Frequency of Publication

CP&CPS 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 will be updated within 24 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 the internal 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 EV SSL Certificates, OV SSL Certificates, DV 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.

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 domain name and IP address（public ONLY）. 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. the content put in this field must reflect the authentic identity of the subject, be meaningful and in line with laws.

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 the OV SSL Certificate, the CN can be the domain name or public IP owned by the subscriber. It is identified and verified with the other information of the subscriber.

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

the subscriber.

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

DN of certificate must be unique for different subscribers in CFCA trust domain, and same DNs cannot be allowed as subscriber's subject name. CFCA can issue more than one certificate using the unique DN for one subscriber. When DN is not unique to different subscribers, the first applicant has the priority to use the DN, and the latter could add more additional information to distinguish from others.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificates issued by CFCA does not contain any trademarks or other

information which may infringe other parties' rights. CFCA don't validate trademark right or legal disputes when processing applications. CFCA has right to refuse applications and revoke any issued certificates when trademark disputes rise.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant shall prove the possession of private key that corresponds to the registered public key. The proving methods include: PKCS#10, other equivalent key identification methods, or other proving methods accepted by CFCA. 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 Organization and Domain Identity

Prior to applying for a certificate under the Global Trust System, the subscriber should provide valid organization identity proof, certifcate application materials including employee or agent authorization 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.

Upon receiving the application, CFCA or the Agency authorized by CFCA will authenticate subscriber identity and store the application materials according to the agreement.

3.2.2.1 Authentication of Organization Identity

The organization shall hold the valididentity documents before applying for a certificate, including but not limited to: business license, legal person code certificate, institution legal person certificate, social organization registration certificate, privatenon-enterprise registration certificate, registration certificate of resident representative office of foreign(regional) enterprise and the government approval, and submitthe certificate application.

The CA or the authorized RA will confirm the actual existence and legality of this organization and confirm the applicant's intention. The authentication procedure is specified as follows.

(1) Check and confirm the valid organization identity document through an authoritative third-party database to ensure that the provided information is consistent with the verification results.

(2) Check the authorization documents authorized by the organization to the authorized representative to handle the certificate and the valid government-issued photo ID of the authorized representative to ensure that the authorized representative is authorized by the organization. The CA can contact the applicant

through a telephone number obtained by Authentication Data Source to confirm the authenticity of some information of the applicant, such as verifying whether a person in the application form is an authorized representative.

(3) Verify the certificate request with the certificate applicant and confirm the true intention of the applicant through SMS, bank payment postscript, etc.

(4) If CA is unable too btain all the required information from a third party, it may entrust a third party to conduct an investigation or request the applicant to provide additional information and supporting materials.

The CA establishes and maintains certificates high risk applicants list and will check the list when accepting certificate applications. For applicants in the list, the CA will reject the application.

3.2.2.2 Verification of DBA/Tradename

Not applicable.

3.2.2.3 Verification of Country

If the certificate subject item contains a country field, CFCA will confirm the host country through the organization approval information provided by the applicant under the section 3.2.2 of CP&CPS.

3.2.2.4 Verification Authentication of Domain Name

For the verification of a domain name, the verified entity may be the

applicant's parent company, subsidiary company or affiliate, and the CA or the authorized RA shall adopt one of the following authentication methods to confirm that the applicant owns the domain name.

(1) As per the procedure of Verification and the Verification and Authentication of Email Address in section3.2.2.9, send a random value by email, and receive a confirming response using the random value to confirm the applicant's ownership of the FQDN. The random value must be sent to the domain name contact email address registered by WHOIS.

(2) As per the procedure of Verification and the Verification and Authentication of Email Addressinsection 3.2.2.9, send a random value by email, and receive a confirming response using the random value to confirm the applicant's ownership of the FQDN. The random value must be sent to the email address identified as the domain name contact or created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster', followed by the at-sign("@"), followed by an authorized domain name.

(3) Confirm the subscriber's ownership of the FQDN by making changes to the agreed information under the "/.well-known/pki-validation" directory.

(4) Confirm the subscriber's ownership of the domain name by confirming the presence of a negotiated random value in a DNSCNAME, TXT or CAA record. Requirements: 1) authorizeddomainname; or 2) an authorized domain name with a prefix starting with underline character.

The random value used in the above validation method remains valid for no

more than 30 days from the time of creation. The CA does not issue SSL Global Server Certificates for domain names in the form of .onion.

3.2.2.5 Verification Authentication of an IP Address

According to the requirements of CA/Browser Forum, the CA does not issue a certificate for a Reserved IP Address marked by IANA or non-routable internal domain names. The CA or an authorized RA shall confirm the applicant's ownership of or control over the IP address using one of the following authentication methods.

(1) Confirm the subscriber's control over the IP address by making changes to the agreed information under the "/.well-known/pki-validation" directory.

(2) Obtain the domain name associated with the IP address by performing a reverse-IP lookup, and then use the method described in Section 3.2.2.4of this CP&CPS to verify the applicant's control over the IP address.

(3) Confirm the applicant's control over the IP address by dialing the telephone number identified as the IP contact and obtaining a response confirming the applicant's request for verifying the IP address.

(4) The subscriber can supply a sealed paper document or email from the ISP showing the IP is allocated by the ISP to the applicant.

The random value used in the above validation methods remains valid for no more than 30 days from the time of creation. The CA does not issue an EV SSL Global Server Certificate for the IP address.

3.2.2.6 Verification Authentication of Wildcard Domain Names

The CA shall confirm the applicant's ownership of and control over the domain name to the right of the wildcard by using one of the validation methods in Section 3.2.2.4 domain name validation method 1, verification method 2 and verification method 4 of this CP&CPS, to ensure that the domain name is clearly assigned to a commercial entity, social organization or governmental agency, and obtained through legal registration.

The CA refuses the certificate application if the domain name to the right of the wildcard is directly a top-level domain name, a public suffix, or the domain name is controlled by the domain name registration management authority, unless the subscriber can prove its rightful control of the entire domain name space.

When necessary, the CA needs to adopt other independent review methods to determine the ownership of the domain name. If the corresponding assistance is needed from the subscriber, the subscriber cannot refuse it for any reason.

3.2.2.7 Data Source Accuracy

The data sources used in the forensic process will be published on the officaial website.

Prior to the use of any data source as a dependent data source, CFCA shall evaluate the reliability, accuracy,and the resistance to alteration or falsification of data source. Following CA/B forum and taking into account the following factors:

1. The age of the information provided;

2. The frequency of updates to the information source;

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

4. The public availability and accessibility of the data;

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

3.2.2.8 Verification Authentication of Email Address

The CA or the authorized RA shall verify the effectiveness and control rights of the applicant's email address. The authentication procedure is specified as follows.

(1) The CA sends a Random Value to the email address, which is generated by the system and isunique.

(2) The applicant must send a confirming response utilizing the Random Value to the CA.

(3) The CA receives the response and shall make sure the received Random Value is the same with the sent one.

3.2.2.9 The random value used in the above validation method remains valid for no more than 30 days from the time of creation.Authentication of DV SSL Certificate Subscriber Identity

If the subscriber applying for an DV SSL Certificate is an individual, it may apply to the CA or anauthorized RA. The DV SSL Certificates can contain IP

addresses and wildcard certificates. When a subscriber applies for a DV SSL Certificate, the following materials shall be submitted:

1. Certificate application form

2. At Least One Organization Information Proof (not applicable to individual subscribers)

3. Applicant's personal identification proof

4. The proof of authorization granted by the organization to the applicant (not applicable to individual subscribers)

5. The proof of having a domain name

6. The proof of having a public IP(domain name is not applicable)

7. Certificate application CSR file

The CA needs to authenticate domain names (IP) and CSR compliance. The authentication procedure is specified as follows.

(1) Through the domain name registration information query (WHOIS) function, obtain the information of the registrant who applies for a domain name certificate, check whether the domain name registrant is consistent with the domain name certificate applicant, and initially verify that the domain name certificate applicant actually owns the domain name. If the domain name applicant is inconsistent with the result of the query (WHOIS), the subscriber may provide a certificate of authorization or the CA may send an email to ask whether it is authorized to the certificate applicant for use.

(2) Confirm the applicant's ownership of the domain name in accordance

with the domain name identification method in Section 3.2.2.4 of this CP&CPS.

(3) Confirm the applicant's ownership of or control over the IP address in accordance with the IP address identification method in Section3.2.2.5 of this CP&CPS.

(4) If one applies for a wildcard domain name certificate, perform wildcard domain name identification in accordance with Section 3.2.2.6of this CP&CPS.

(5) The identification of the CSR file mainly includes whether the information in the CSR is consistent with the application information in the application form, whether it conforms to relevant specifications, such as the order of the DN, and whether it has aprivate key.

(6) Check the CAA records in accordance with requirements

3.2.2.10 Authentication of OV SSL Certificate Subscriber Identity

If the subscriber applying for an OV SSL Certificate is an organization, it may apply to the CA or an authorized RA. The OV SSL Certificates can contain wildcards, IP addresses, or multiple domain name certificates. When a subscriber applies for an OV SSL Certificate, the following materials shall be submitted:

1.Certificate application form

2.At Least One Organization Information Proof

3.Applicant's personal identification proof

4.Proof of authorization granted by the organization to the applicant

5.Proof of having a domain name

6.Proof of having a public IP (domain name is not applicable)

7.Certificate application CSR file

In addition to the identification of the subscriber, the CA also needs to authenticate domain names (IP) and CSR compliance. The authentication procedure is specified as follows.

(1) Authentication of organization identity in accordance with the requirements of Section 3.2.2.1 of this CP&CPS.

(2) Through the domain name registration in formation query (WHOIS) function, obtain the information of the registrant who applies for a domain name certificate, check whether the domain name registrant is consistent with the domain name certificate applicant, and initially verify that the domain name certificate applicant actually owns the domain name. If the domain name applicant is inconsistent with the result of the query (WHOIS), the subscriber may provide a certificate of authorization or the CA may send an email to ask whether it is authorized to the certificate applicant for use.

(3) Confirm the applicant’s ownership of the domain name in accordance with the domain name identification method in Section 3.2.2.4 of this CP&CPS.

(4) Confirm the applicant's ownership of or control over the IP address in accordance with the IP address identification method in Section 3.2.2.5 of this CP&CPS.

(5) If one applies for a wildcard domain name certificate, perform wildcard domain name identification in accordance with Section 3.2.2.6 of this CP&CPS.

(6) The identification of the CSR file mainly includes whether the information in the CSR is consistent with the application information in the application form, whether it conforms to relevant specifications, such as the order of the DN, and whether it has a private key.

(7) Check the CAA records in accordance with requirements.

3.2.2.11 Authentication of EV SSL Certificate Subscriber Identity

If the subscriber applying for an EV SSL Certificate is an organization, it may apply to the CA or an authorized RA. The EV SSL Certificate application can only be the domain name of the WEB server, and the domain name can not contain wildcards. The application for the IP address is not accepted. The EV SSL Certificates can include multiple domain name certificates.

Applicant subscribers can only be organizations such as Government Entity, Business Entity, and Private Organization. And the applicant organizations need to meet the following conditions:

1.Government Entity shall meet the following conditions:

(1)Approved by the superior in accordance with its functions;

(2)The authorized representative of the unit must be specified in the subscriber application materials;

(3)In a country where CA is allowed to issue a certificate;

(4)Not on any denial list or prohibited list (such as the trade embargo) by the government.

2.Business Entity shall meet the following conditions:

(1)A legal organization acknowledged by the local regulatory body;

(2)Not listed in the “closed”, “invalid” or “expired” list of the regulatory body;

(3)The authorized representative of the unit must be specified in the subscriber application materials;

(4)Have a fixed place of business;

(5)The country in which Business Entity and its authorized representative reside allows the CA to issue a certificate;

(6)Business Entity and its authorized representative are not on any denial list or prohibited list (such as the trade embargo) by the government.

3.Private Organization shall meet the following conditions:

(1)A legal organization acknowledged by the local regulatory body;

(2)Not listed in the “closed”, “invalid” or “expired” list of the regulatory body;

(3)The authorized representative of the unit must be specified in the subscriber application materials;

(4)Have a fixed place of business;

(5)In a country where CA is allowed to issue a certificate;

(6)Not on any denial list or prohibited list (such as the trade embargo) by the government.

4.The role that the applicant or ganization shall have:

Certificate Requestor: handling personnel of the application unit

Certificate Approver: the person in charge of the applicatio nunit

Contract Signer: Signatory of the application agreement

Applicant Representative: In the case that the CA and the applicant are related parties, and both parties have applicable guidelines for the use of EV certificates, the applicant must set an application agent to represent the applicant to accept the guidelines for the use of certificates.

The certificate applicant organization can authorize one person or multiple people to fulfil all the roles. Above roles must be employees or authorized agents of the applicant. The applicant shall confirm that the information of the application role is true and accurate, and make a statement in the way approved by CA (including but not limited to the registered official seal, registered legal person's name seal, role signature, etc.). For the false information of the application role, the CA has the right to refuse the application and withdraw the issued certificate.

5.The domain name of the applicant organization:

(1)The applicant organization owns the domain name ownership or exclusive use rights and is aware of its ownership or exclusive use rights to the domain name;

(2)Domain name registration information shall be disclosed in the WHOIS database.

6.When a subscriber applies for an EV SSL Certificate, the following materials shall be submitted:

(1)EV Certificate application form

(2)At Least One Organization Information Proof

(3)Certificate Requestor's identification proof

(4)Proof of authorization granted by the organization to Certificate Requestor

(5)Proof of company' sexistence

(6)Proof of having a domain name

(7)Certificate application CSR file

The authentication procedure of the EV SSL certificate application by the CA is as follows:

(1)Subscriber identity authentication

a.Verify the legality of the applicant organization

Query the registration code(such as unified social credit code) of the applicant organization through Authentication Data Source for EV Certificates; verify the identity information and registered address of the applicant;

It must be verified directly by a qualified independent source of information.

b.Content of organization verification

Whether the identity information of the applicant organization exists;

Whether the identity information of the applicant organization is accurate;

Whether the business address provided by the applicant organization is consistent with the registered address in the registration document (such as business license).

c.Verify operational existence of the applicant organization

Through Authentication Data Source for EV Certificates, query the registration code of the applicant organization to verify its operational existence or query the bank capital verification report provided by the applicant organization to verify its operational existence status.

d.Authentication of EV certificate applicant's principal individua

EV certificate requestor (When individual businesses apply for EV certificate, the certificate request or must be the operator himself) must be verified by face-to-face (video) methods;

Verify identity information through the Ministry of Public Security identity verification platform;

Contact the personnel department of the application organization by dialing the fixed line telephone (must be the company phone number obtained from the authentication data source) to confirm the identity and authorization of Certificate Requestor, Certificate Approver and Contract Signer.

(2)Domain name authentication

Confirm the applicant's ownership of the domain name in accordance with the domain name identification method in Section 3.2.2.4 of this CP&CPS.

(3)CSR file authentication

Verify the content of the CSR file submitted by the subscriber, check whether the information in the CSR is consistent with the information in the applicationform, whether it complies with the relevant specifications, and verify whether it has aprivate key.

3.2.2.12 Authentication of EV SSL/ OV SSL/DV SSL Certificate Subscriber Identity

CFCA issues certificates for subscribers and deliver the public key certificates to the subscribers via proper ways (such as emails).

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, the organization shoud be responsibleto ensure all roles' information are correct and declared by CFCA admitted measures. 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 CFCA EV OCA, CFCA OV OCA, CFCA DV OCA, CFCA EV ECC OCA, CFCA OV ECC OCA, CFCA DV ECC OCA, CFCA EV RSA OCA, CFCA OV RSA OCA, CFCA DV RSA OCA. No other organization is delegated with this function.

3.3 Identification and Authentication for Re-key Requests

"Renew" is the only supported for certificated key pair validity update in CFCA global trust system.

1. Certificate Renew

(1) when the subscriber certificate is damaged or lost i.g storage broken;

(2) subscriber suspects unsafe status of original certificate and key pairs;

(3) other CFCA admitted reasons.

To those who apply renew in twelve months after the first-time issuance, subscriber and the information has not changed, don't need to submit role validation materials. CFCA only validate the first-time application information and validate the new CSR and Domain at the same time. Revalidation and requirements are need and same as the first-time application when renew happens after twelve months.

Certificate renew is the application for the issuance of a new certificate within the one month prior to the expiration of the existing certificate. For EV/OV/DV SSL 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.

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

During the one month before the expiry date, CFCA reminds the subscriber to apply for certificate renew via appropriate channels.

To apply for certificate renew 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 renew request, and agree to bear corresponding responsibility. Upon receiving the certificate renew 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 renewed, 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, the old certificate would be revoked after the renew operation. Expired certificate could only apply for new issuance, the new certificate will only be valid for one validity period. The overdued certificate won't be revoked after rekey.

3.3.1 Identification and Authentication for Routine Re-key

Same as Section 3.3.

3.3.2 Identification and Authentication for Re-key After Revocation

CFCA treats the re-key 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 4.9.3.

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 CP&CPS (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 authorized agency 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 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. RAs verify the identity of the subscribers according to the requirements stated in Section 3.2.2. CFCA issue certificates to subscribers who have undergone the verification. CFCA and authorized agency should properly retain subscribers' application documents,

archive relevant information at CFCA within appropriate time limit, and practice the responsibilities and obligations stated in this CP&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 agency with competency of the language in question. CFCA will review the authentication results of the agency and ensure that the self-assessment requirements in the Certificate standards are met.

5) According to CA/B Forum Baseline Requirements, CFCA will check CAA information of the domain name in customers' requests since September 1st, 2017. Since May 2018, CT Log would be embedded in EV/OV/DV SSL certificate. Since September 1, 2020, the Maximum Lifetime of EV/OV/DV SSL Certificates are 398 days or less.

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.

4.2.4 Certification authority authorization

CFCA follows CA/B Forum BR requirements to perform DNS CAA record checks on all subject names and domain names in alternate names in certificate applications.

CFCA will issue a certificate to the certificate applicant within the validity period of the CAA record(the TTL of the CAA record,or 8 hours,whitchever is greater).If the validity period of the CAA record is expired,we will re-check the CAA.

CFCA processes the "issue," "issuewild," "iodef" attribute tags in CAA records according to the regulations of RFC8659.

When processing the property tags in CAA records, CFCA will not act on the contents of the iodef property tag. CFCA respects the critical flag and will not issue a certificate if they encounter an unrecognized property with this flag set.

CFCA will refuse to issue a certificate when the CAA response data has the "issue", "issuewild" tags, and the tag content does not contain “cfca.com.cn".

CFCA are permitted to treat a record lookup failure as permission to issue if:

1. The failure is outside the CA's infrastructure;

2. The lookup has been retried at least once;

3. The domain's zone does not have a DNSSEC validation chain to the ICANN root.

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 CP&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 CP&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 or OCSP provided by 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 Renewal

4.6.1 Circumstances for Certificate Renewal

The Certificate renewal refers to the issuance of a new certificate to a subscriber without changing the subscriber's public key or any other information in the certificate. No certificate Renewal service is provided by CFCA. We recommends subscribers to use the certificate re-key service preferentially. For details, see Section 4.7 of this CP&CPS.

4.7 Certificate Re-key

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

4.7.1 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.

4.7.2 Who May Request Rekey

Subscribers holding certificates issued by CFCA may request certificate

rekey.

4.7.3 Processing Certificate Rekey Requests

Same as Section 3.3;

4.7.4 Notification of New Certificate Issuance to Subscriber

Same as Section 4.3.2;

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Same as Section 4.4.1;

4.7.6 Publication of the Rekeyed Certificate by the CA

Same as Section 4.4.2;

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Same as Section 4.4.3;

4.8 Certificate Modification

No certificate modification service is provided by CFCA.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

CFCA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

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

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

3. CFCA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;

4. CFCA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate(such as a Debian weak key, see https://wiki.debian.org/SSLkeys);

5. CFCA obtains evidence that the validation of domain authorization or control for any Fully‐Qualified Domain Name or IP address in the Certificate should not be relied upon.

CFCA should revoke the certificate within 24 hours if one or more of the following occurs, and the certificate must be revoked within 5 dyas.

1. CFCA is informed that the certificate no longer complies with the relevant requirements of Section 6.1.5 and 6.1.6 of the Baseline Requirements;

2. CFCA obtains evidence that the certificate was misused;

3. CFCA is made aware that a subscriber has violated one or more of its material obligations under the subscriber agreement and CP&CPS;

4. 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 domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name registrant has failed to renew the domain name);5. When the CA has evidence that the subscriber has lost the right to use the domain name in the certificate, or the subscriber has failed to renew the right to use the domain name;

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

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

8. 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;

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

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

revocation support for the Certificate;

11. 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;

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

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

14. 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).

15. Other situations stipulated in relevant laws and regulations.

4.9.2 Entity request certificate revocation

The subscribers, RA、CFCA can initiate revocation. Additionally, relying parties, application software suppliers,other third parties may submit certificate problem reports informing CFCA of reasonable grounds to revoke the

certificates.All subscribers holding CFCA certificates can request revocation.

4.9.3 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.

4.9.3.1 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.

CFCA receive and process revocation request for 7*24 hours.

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.

4.9.3.2 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.

4.9.4 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.

4.9.5 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.

If the situation in the first part of chapter 4.9.1 occurs, CFCA will revoke the

certificate within 24 hours.

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency

CFCA differentiate CRL updating according to the systems that issue the certificates. CRL information issued by CFCA EV OCA, CFCA OV OCA, CFCA DV OCA, CFCA EV ECC OCA, CFCA OV ECC OCA, CFCA DV ECC OCA, CFCA EV RSA OCA, CFCA OV RSA OCA, CFCA DV RSA OCA will be updated within 24 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.

4.9.8 Maximum Latency for CRLs

The maximum latency fo CRL publication is 24 hours.

4.9.9 Online Revocation/Status Checking Availability

OCSP service is avaible for 7*24.

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 RFC6960 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.

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 RFC6960 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.

4.9.10 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.

4.9.11 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.

4.9.12 Certificate Suspension

Not applicable for the certificates under the Global Trust System.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status is available through the OCSP service of CFCA.

4.10.2 Service Availability

Certificate status inquiry service is provided 7*24 by the CFCA.

4.11 End of Subscription

The subscription is ened when：

1. The certificate has expired;

2. The certificate is revoked.

4.12 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 Certification Authority Management Operational and Physical 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 must pass the audit and multi access system. The electromagnetic shielding of the computer room meets the Level “C” requirements of the GJB 5792-2006 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. The whole environment 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.

5.1.9 Phydical Control on CFCA Timestamp Server

CFCA control and run the timestamp server indenpendently, the private key is stored in encryption machine and make sure the encryption machine satisfies FIPS-140-2 requirements. The time resource of CFCA timestamp service is BDT which is originally from National Time Service Center of Chinese Academy of Sciences UTC.

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 above said 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 employment 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 / ISO 27001 QCMS and ITMS training and CP&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;

Log entries include the following elements: date and time of the entry; serial or sequence number of entries; 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. CP&CPS 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 librarian to manage the archives. Policies have been formulated to restrict the access to the paper archives to authorized personnel.

5.5.4 Archive Backup Procedures

Database, operation systems, and logs are backed up.

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.

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).

Generate 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 disastrous 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 disastrous 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 7*24 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 7*24 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 occurrence 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 termination 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 business 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.

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 proper ways (such as 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 EV ROOT—RSA-4096/SHA-256

CFCA EV OCA-RSA-2048/SHA-256

CFCA OV OCA-RSA-2048/SHA-256.

CFCA DV OCA—RSA-2048/SHA-256

CFCA Global ECC ROOT —ECC-384（NIST P-384）/SHA-384

CFCA EV ECC OCA—ECC-256（NIST P-256）/SHA-256

CFCA OV ECC OCA—ECC-256（NIST P-256）/SHA-256

CFCA DV ECC OCA—ECC-256（NIST P-256）/SHA-256

CFCA Global RSA ROOT —RSA-4096/SHA-256

CFCA EV RSA OCA—RSA-2048/SHA-256

CFCA OV RSA OCA—RSA-2048/SHA-256

CFCA DV RSA OCA—RSA-2048/SHA-256

The key size of subscriber keys is RSA-2048 or ECC-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

OV SSL Certificate	sha256RSA sha256ECDSA	RSA-2048、ECC-256	1	Digital signature, Non-repudiation, Key agreement, Key encrypherment	Server authentication
EV-SSL Certificate	sha256RSA sha256ECDSA	RSA-2048、ECC-256	1	Digital signature, Key encrypherment	Server authentication
DV-SSL Certificate	sha256RSA sha256ECDSA	RSA-2048、ECC-256	1	Digital signature, Key encrypherment	Server authentication

Note: Since September 1, 2020, the Maximum Lifetime of EV/OV/DV SSL Certificates are 398 days or less.

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, ECC, Diffie Hellman, can be used. Optional RSA sizes include 2048 and 4096 bits. Compatible symmetric

algorithms include SDBI, DES, Triple-DES, IDEA, RC2, RC4, RC5. Strong encryption of 128 bits is supported. Compatible HASH algorithms include MD2, MD5, SHA1, SDHI, SHA256 and SHA384.

The public key algorithms for the cryptographic devices used in the CFCA Global Trust System include RSA-2048, RSA-4096, ECC-256; and HASH algorithms include SHA1(stop at 1 JAN 2016) SHA256 and SHA384. 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 cyrptographic 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 storaged 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 two fragments that stored in three IC cards. Each of the IC cards is held 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 two shareholders out of the three. 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 magnetic 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 established 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 measures. 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 25 years. The validity period of EV/OV/DV SSL certificates is up to two years. (Since September 1, 2020, the Maximum Lifetime of EV, OV and DV SSL Certificates are 398 days or less).

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.

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 Security Controls

6.7.1 Root Key Controls

The root key generation ceremony should be witnessed by a qualified auditor, who then issue a report opinion 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 and ISO 27001 ITMS standards. Core data is backed up 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 Administration 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, split 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, TSA, 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 fields. Please refer to Appendix B for the fields contained in Global Trust 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, this field is serverAuth.

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.

OV SSL certificates, OV CodeSign certificate, EV SSL certificates, EV CodeSign certificate must contain this field.

For OV CodeSign Certificate and EV CodeSign certificates, this field will contain id-on-permanentIdentifier (OID 1.3.6.1.5.5.7.8.3)

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/RSA2048, SHA-256/RSA4096, ECC-256/SHA-256, ECC-384/SHA-384 algorithms, and comply with RFC 3280 standards.

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 according to RFC 5280.All information contained in the certificate is verified by the CFCA.

The DN of the certificates issued by the OV system include the following 7 parts:

1、 CN：The real name of the Entity，for SSL certificates, this item should be

the Domain Name or public IP address.

2、 OU：Optional. To indicate the department name of the entity or effective information confirmed by the subscriber. If OU exists, CFCA must verify this part. From September 1, 2022, certificates containing the OU field will no longer be reviewed and issued.

3、 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.

4、 L：Optional. Indicates the city of company location for registration or operation, if 'S' required, 'L' oprional;

5、 S：Optional. Indicates the provice or state of company location for registration or operation, if 'L' required, 'O' oprional;

6、 C：indicates the country or region of the company location.

The country, province and city names in the DN must be those listed in the standards released by authorities (e.g. ISO 3166).

As to the certificates issued under CFCA Global Trust Certificates, 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 Global Trust Certificates .

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, 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.

OV SSL Certificate OID is 2.16.156.112554.4.1.

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 Profile

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

7.3 OCSP Profile

CFCA Global Trust system provides Online Certificate Status Protocol services.

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.

7.3.1 Version Number(s)

The OCSP v1 as defined in FRC 6960.

7.3.2 OCSP Extensions

OCSP extensions are not used.

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 CP&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 CP&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 CP&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 CP&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 CP&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 CP&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 CP&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 CP&CPS, 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 CP&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 CP&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、 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.

3、 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.

4、 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.

5、 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.

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

9.6.3 Subscriber Representations and Warranties

Subscribers represent and warrant that:

1, Subscriber 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, in accurate or incomplete information submitted intentionally or accidentally by subscriber, or subscriber failed to inform

CFCA and the original RA the information changes, are borne by subscriber.

2, Subscriber shall use software obtained through legitimate means.

3, the subscriber should generate key pairs in safe ways to avoid any loss or exposure. The subscriber should keep the public key certificate and private key in right ways. The subscriber shoud be responsible for any mis-use of private key and pin code for any purpose. In case of theft, fraudulent use of a digital certificate private key and password caused by intentional or negligent actions of the subscriber, subscriber shall be liable for the result.

4, the subscriber shall take the necessary measures to guarantee the safety of certificate, private key and the associated password, including storage, usage and backup. If the subscriber's digital certificate private key and password leaked or lost, or the subscriber does not want to continue to use a digital certificate, or the subject of subscriber does not exist anymore, subscribers or legal rights holder should inform the original RA and apply for revoke immediately, the relevant procedures comply with RA requirements.

5, the subscriber should use the certificate in legal purpose.

6, subscriber bear the responsibilities for using the certificates:

① use of certificates should comply with all applicable laws and regulations;

② use of certificates should be consistent with the intention of the subscriber, or just handle authorized affairs;

③ use of certificates should comply with the this CP&CPS's terms and conditions of use.

7.subscriber should ensure all information in the certificate correct after receive the certificate.

8, subscriber should know the certificate wouldn't be valid once revoked.

9, subscriber should know CFCA has right to rovke the certificate if CFCA find the certificate is used in illegal ways.

10, If subscriber harm the interests of the CFCA, subscriber will indemnify CFCA for losses and damages. Circumstances include, but are not limited to:

①Falsehood/incompleteness/misrepresentation of information provided by the subscriber on the certificate application. Subscribers failed to inform CFCA timely when the information change.

② Subscriber knows its digital certificate's private key has been compromised or may have been compromised without timely inform the relevant parties, and cease use;

③ subscriber failed in fulfill other relevant stipulations of this CP&CPS.

11, subscriber should pay for the certificate service on time.

12, CFCA has right to require subscriber to replace certificate with the development of technology. Subscriber should ask for replacement after reveive the notification. Subscriber would take any results itself for not replacing in time.

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 CP&CPS and the usage of certificates and use the certificates within the scope stipulated by this CP&CPS.

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

9.6.5 Representations and Warranties of Other Participants

The unidentified participants should observe the stipulations in this CP&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 partner's ultra vires behavior or other mistakes.

9.8 Limited Liability

If according to this CP&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

According to "Electronic Signature Law of the People's Republic of China", CFCA shall compensate the subscriber or relying party, who suffers loss caused by the certification service provided by CFCA. However, CFCA shall not be deemed at fault 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 CP&CPS filed to the competent department, and shall not be required to bear any compensation and reimbursement responsibility towards the subscriber or relying party.

The following is not liable for compensate, whether it has infringed this agreement or not:

①Any 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;

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

③ losses due to non-CFCA behavior caused;

④ loss caused by force majeure, such as strikes, wars, disasters, viruses and other malicious code.

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

9.10 Term and Termination

9.10.1 Term

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

CP&CPS is terminated.

9.10.2 Termination

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

The CP&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 CP&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 CP&CPS, please contact CFCA at 010-80864996.

9.12 Amendments

CFCA is entitled to amend this CP&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 “CP&CPS Approval Procedure”.

9.12.2 Notification Mechanism and Period

CFCA reserves the right to amend any term and provision contained in this CP&CPS without notice. But the revised CP&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 CP&CPS Must be Amended

CFCA shall amend this CP&CPS if the rules, procedures and relevant technologies stated in this CP&CPS can no longer meet the demands of CFCA’s certification business; the governing laws and regulations of this CP&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 CP&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 CP&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 authorities. In the event that a clause or provision of this CP&CPS is held to be illegal, unenforceable or invalid by a court of law or other tribunal having authority, the remainder of the CP&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 CP&CPS renders invalid the written or verbal explanations on the same topics during the previous or same periods. The CP&CPS, 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 CP&CPS is held to be illegal, unenforceable or invalid by a court of law or other tribunal having authority, the remainder of the CP&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 Certificates (From http://www.cabforum.org.). Should there be any inconsistency between the CP&CPS and the above Guidelines, the latter shall prevail.

Appendix A 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 Protocol
CP	Certificate Policy
CPS	Certificate Practice Statement
CSR	Certificate Signature Request
IETF	The Internet Engineering Task Force
DNS	Domain Name System
FIPS	Federal Information Processing Standards
EV	Extended Validation

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 identity 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 confidentiality).
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 identifier 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 Global Trust Certificate Format

Format of EV SSL Certificates			
Field	**Value**		
Version	V3		
Serial Number	Contains 20 non-serial digits		
Algorithm	SHA256RSA	SHA256RSA	SHA256ECDSA
Issuer	CN = CFCA EV OCA O = China Financial Certification Authority C = CN	CN = CFCA EV RSA OCA O = China Financial Certification Authority C = CN	CN = CFCA EV ECC 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	Compulsory and contains only domain name
	OU = IT department	Name of the department (No more OUs from September 1, 22022)	Name of the department (No more OUs from September 1, 22022)
	O = China E-banking network	Legal organization name. If unofficial name is used, it should correctly reflect the organization name and no misleading interpretation are caused. If the name exceeds 64 bytes, abbreviation should be used, but no misleading interpretation should be caused.	Legal organization name. If unofficial name is used, it should correctly reflect the organization 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.	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	Country Code
	SERIALNUMBER = 110000006499259	ID number (eg. Organization code, Business certificate code, tax registration code). Or date of establishment if no registered ID number provided.	ID number (eg. Organization 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	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	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）	RSA（2048）	ECC（256）
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		
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	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)		
Subject Alt Name	Domain		

Format of OV SSL Certificates			
Field	**Value**		
Version	V3		
Serial Number	Contains 20 non-serial digits		
Algorithm	SHA2RSA	SHA256RSA	SHA256ECDSA
Issuer	CN = CFCA OV OCA O = China Financial Certification Authority C = CN	CN = CFCA OV RSA OCA O = China Financial Certification Authority C = CN	CN = CFCA OV ECC OCA 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	Compulsory and must be domain name or external IP address
	OU = IT Department	Department name（non compulsory） (No more OUs from September 1, 22022)	Department name（non compulsory） (No more OUs from September 1, 22022)
	O = China E-banking network	Legal organization name. If unofficial name is used, it should correctly reflect the organization name and no misleading interpretation are caused. If the name exceeds 64 bytes, abbreviation should be used, but no misleading interpretation should be caused.	Legal organization name. If unofficial name is used, it should correctly reflect the organization 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.	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	Country Code
Public Key	RSA（2048）	RSA（2048）	ECC（256）

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/ovoca/ovoca.cer		
Authority Key Identifier			
Basic Constraints	Subject Type=End Entity Path Length Constraint=None		
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.156.112554.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us/us-11.htm		
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.cfca.com.cn/ovoca/RSA/crl1.crl	CRL distribution point	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)		
Subject Alt Name	Public IP or Domain		

Format of DV SSL Certificates			
Field	**Value**		
Version	V3		
Serial Number	Contains 20 non-serial digits		
Algorithm	SHA2RSA	SHA256RSA	SHA256ECDSA
Issuer	CN = CFCA DV OCA O = China Financial Certification Authority C = CN	CN = CFCA DV RSA OCA O = China Financial Certification Authority C = CN	CN = CFCA DV ECC OCA 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	Compulsory and must be domain name or external IP address
Public Key	RSA（2048）	RSA（2048）	ECC（256）
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/ovoca/ovoca.cer		
Authority Key Identifier			
Basic Constraints	Subject Type=End Entity Path Length Constraint=None		

Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.156.11255 4.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.cfca.com.cn/us /us-11.htm		
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.cfca.com.cn/evoca/RSA/crl1.crl	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.cfca.com.cn/eccroot/RSAs/crl1.crl	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.cfca.com.cn/eccroot/ECC/crl1.crl
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)		
Subject Alt Name	Public IP or Domain		

Appendix C Data Source Accuracy

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.

Appendix D CAs constrained by CFCA Global Trust System CP&CPS 4.4

NO	Root CA	Root CA Algorithms	Intermediate CA	Intermediate CA Algorithms
1	CFCA EV Root	RSA4096/SHA256	CFCA EV OCA	RSA2048/SHA256
			CFCA OV OCA	RSA2048/SHA256
			CFCA DV OCA	RSA2048/SHA256
2	CFCA Global ECC ROOT	ECC-384/SHA384	CFCA EV ECC OCA	ECC-256/SHA256
			CFCA OV ECC OCA	ECC-256/SHA256
			CFCA DV ECC OCA	ECC-256/SHA256
3	CFCA Global RSA ROOT CA1	RSA4096/SHA256	CFCA EV RSA OCA	RSA2048/SHA256
			CFCA OV RSA OCA	RSA2048/SHA256
			CFCA DV RSA OCA	RSA2048/SHA256