CFCA Certificate Policy and Certification Practice Statement for Global Trusted System

（CFCA Global-Trust CP/CPS）

V4.10

November 3, 2025

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 descriptions, update content according to the RFC 3647; add DV SSL**	**Bi Xinlong**	**Security Committee**	**July 2021**

		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
4.5	Amend	Modify policy management contact information; revise some content descriptions	Wang Ruohan		September 2023
4.6	Amend	Adjust the definitions and abbreviations in the appendix to Section 1.6; revise organization identity authentication; revise domain name authentication; revise certificate approval and rejection; revise certificate issuance to add linting; revise certificate configuration requirements; revise audit and evaluation	Qiu Dawei Li Kairui Gao Peiyan Zhao Sha	Security Committee	August 30, 2024
4.7	Amend	Add CPR Contact Form to Section 1.5.2 and fix some typos in 11.3	Song Xinlei Xu	Security Committee	May 30, 2025

			Shengchen Gao Peiyan		
4.8	Amend	Modify DCV and revise some content descriptions	Song Xinlei Xu Shengchen Gao Peiyan Zheng Xiaojuan	Security Committee	July 21, 2025
4.9	Amend	Self Assessment amendment	Song Xinlei Xu Shengchen Gao Peiyan Zheng Xiaojuan	Security Committee	October 25, 2025
4.10	Amend	Adjust ROOT/Subordinate CA names	Song Xinlei Gao Peiyan	Security Committee	November 3, 2025

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 combined Certificate Policy ("CP") and Certification Practice Statement ("CPS") document ("CP/CPS") is the certificate policy and certification practice statement for CFCA Global Trusted System.

This CP/CPS conforms to the Electronic Signature Law of the People's

Republic of China, the Cryptography Administration of Electronic Certification Services by OSCCA, the 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, WebTrust, the current version of the Guidelines forforforfor The Issuance And Management Of Extended Validation Certificates and the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates published at <https://www.cabforum.org> by CA/B Forum and other common practices of CAs.

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.

If any inconsistency exists between this document and the normative provisions of an applicable industry guideline or standard ("Applicable Requirements"), then the Applicable Requirements take precedence over this CP/CPS.

1.2 Document Name and Identification

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

1.2.1 Certificate Policy Identification

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

No	Type of OID	OID	Description
1	Document Identifier	2.16.156.112554.2	CFCA Global Trust System CP/CPS
2	Certificate Identifier	2.16.156.112554.3	EV SSL Cert
3	Certificate Identifier	2.23.140.1.1	EV SSL Cert (required by Baseline Requirements)
4	Certificate Identifier	2.16.156.112554.4.1	OV SSL Cert
5	Certificate Identifier	2.23.140.1.2.2	OV SSL Cert (required by Baseline Requirements)
6	Certificate Identifier	2.16.156.112554.4.3	DV SSL Cert
7	Certificate Identifier	2.23.140.1.2.1	DV SSL Cert (required

			by Baseline Requirements)
8	Extension Field Identifier	1.3.6.1.4.1.11129.2.4.2	Certificate Transparency (require by main Root CA programs)

1.2.2 Revision History

Ver.	Action	Description	Effective Date
1.0	**Draft, review and approve the first version.**		**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.**	
	Amend	**Amend related content according to the review of the Security Committee on April 7, 2013.**	**April 2013**
2.0.1	**Amend**	**Amend / Add related content in order to comply with latest Baseline Requirement**	**March 2014**
2.1	**Amend**	**Amend related content in order to resolve issue raised in Mozilla Public discussion in June 2014**	**Nov 2014**
3.0	**Amend**	**Amend related content, add OV CodeSign, OV SSL Certificate,EV codesign related sections**	**Aug 2015**
3.1	**Amend**	**Amend related content, Amend OV CodeSign, OV SSL Certificate,EV codesign related sections**	**June 2015**
3.2	**Amend**	**Related section amended according minutes on Security Committee on June 24th, 2016**	**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.**	**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**	**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**	**July 2020**
4.2	**Amend**	**Update Mozilla Root store Police， BR and EV Guidelines compliance descriptions, update content according to the RFC 3647；add DV SSL Certificate content；Text correction**	**July 2021**
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**	**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**	**November 2022**
4.5	**Amend**	**Modify policy management contact information; revise some content descriptions**	**September 2023**
4.6	**Amend**	**Adjust the definitions and abbreviations in the appendix to**	**August 30, 2024**

		Section 1.6; revise organization identity authentication; revise domain name authentication; revise certificate approval and rejection; revise certificate issuance to add linting; revise certificate configuration requirements; revise audit and evaluation	
4.7	**Amend**	**Add CPR Contact Form to Section 1.5.2 and fix some typos in 11.3**	**May 30, 2025**
4.8	**Amend**	**Modify DCV and revise some content descriptions**	**July 21, 2025**
4.9	**Amend**	**Self Assessment amendment**	**October 25, 2025**
4.10	**Amend**	**Adjust ROOT/Subordinate CA names**	**November 3, 2025**

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 Registration 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 G2, CFCA OV ECC OCA G2, CFCA DV ECC OCA G2, CFCA EV RSA OCA G2, CFCA OV RSA OCA G2, CFCA DV RSA OCA G2 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 digital certificates issued by CFCA.

It should be noted that, "Subscriber" and "Subject" are two different terms 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 refers 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 trusted 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

Other entities not mentioned above that participate in the provision of certificate services within the entire CFCA and its service architecture.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

CA	Server
CFCA EV OCA	EV SSL Certificate(RSA)
CFCA OV OCA	OV SSL Certificate(RSA)
CFCA DV OCA	DV SSL Certificate(RSA)
CFCA EV ECC OCA G2	EV SSL Certificate(ECC)
CFCA OV ECC OCA G2	OV SSL Certificate(ECC)
CFCA DV ECC OCA G2	DV SSL Certificate(ECC)
CFCA EV RSA OCA G2	EV SSL Certificate(RSA)
CFCA OV RSA OCA G2	OV SSL Certificate(RSA)
CFCA DV RSA OCA G2	DV SSL Certificate(RSA)

CFCA EV ROOT, CFCA Global ECC ROOT G2 and CFCA Global RSA ROOT G2 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 G2 and CFCA EV ECC OCA G2.

Available key sizes are RSA-2048, RSA-4096, ECC-256 (NIST P-256).

1.4.1.2 CFCA OV SSL 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 G2 and CFCA OV ECC OCA G2.

Available key sizes are RSA-2048, RSA-4096, ECC-256 (NIST P-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 G2 and CFCA DV ECC OCA G2.

Available key sizes are RSA-2048, RSA-4096, ECC-256 (NIST P-256).

1.4.2 Prohibited 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.

Certificates issued under the CFCA Global Trust System cannot be used in the following areas: Any application system that violates national or local laws and regulations.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization administering this document is the Business Operation Management 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 Person

Any question on this CP/CPS, please contact the Business Operation Management Department:

Tel: 010-80864610	Fax: 010-63555032
E-Mail: cps@cfca.com.cn	Address: 8th Floor, Parkson North Building, No. 37 Financial Street, Xicheng District, Beijing, P.R. China

For Certificate Problem Reports, please contact CFCA by filling the webform on our website: https://cloudpki.cfca.com.cn/cpr.

1.5.3 Person Determining 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 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 Business Operation Management 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 published 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 Business Operation Management Department coordinates related parties in the publication.

The online publication of the CP/CPS follows the *CFCA Website Management Methods*. CP/CPS published in other forms should be consistent with the one posted on the website. The Business Operation Management 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 Business Operation Management 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 Legal Compliance Department 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 Business Operation Management Department within 20 days following the publication.

1.6 Definitions and Acronyms

1.6.1 Definitions

Project	Concept Definition
Electronic certification service agency	An authority trusted by subscribers that is responsible for creating, issuing, and managing public key certificates and can sometimes create keys for subscribers.
Registration Agency	For certificate subscribers, responsible for the application, approval and management of subscriber certificates.
Digital Certificates	An electronic file digitally signed by a CA that contains the public identity information and public key of the digital certificate user.
Certificate Revocation List	A list of revoked certificates issued and published by a certification authority (CA)
Online Certificate Status Protocol	A protocol issued by the IETF for checking the status of digital certificates.
Certificate Policy	A named set of rules that indicate the applicability of a certificate to a particular group and/or type of application with similar security requirements.
Electronic Certification Business Rules	A statement about the business practices used by the electronic certification service provider in issuing, managing, revoking, or renewing certificates (or renewing the keys in certificates).
subscriber	The entity requesting the certificate.
Relying Party	A relying party is an individual or organization that relies on the basic trust relationship proved by the certificate and conducts business activities based on it.构。
Private Key	In an asymmetric cryptographic algorithm, a secret key that can only be used by its owner.
Public Key	A key that can be made public in an asymmetric cryptographic algorithm.
Unique identification name	In the subject name field of a digital certificate, the X.500 name used to uniquely identify the subject of the certificate. This field needs to be filled with content that reflects the true identity of the subject of the certificate, has practical significance, and does not conflict with the law.
RFC5280	RFC5280 is a profile for X.509 public key infrastructure certificates and certificate revocation lists.
RFC6960	RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
X.509 Protocol	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, X.509 is the format standard for public key certificates in cryptography.
X.500 Protocol	The naming convention for digital certificates generally uses the X.500 format.
Network Perspective	Related to Multi-Perspective Issuance Corroboration. A system

	(e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.
Primary Network Perspectiv	The Network Perspective used by the CA to make the determination of 1) the CA’ s authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant’ s authority and/or domain authorization or control of the requested domain(s) or IP address(es).
Multi-Perspective Issuance Corroboration	A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.
Authorized Ports	One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

1.6.2 Acronyms

project	Abbreviation 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	Certification Practice Statement
CSR	Certificate Signature Request
IETF	The Internet Engineering Task Force
DNS	Domain Name System
FIPS	Federal Information Processing Standards
EV	Extended Validation
DN	Distinguished Name

1.6.3 References

1. http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf RFC3647 standard published by the Internet Engineering Task Force (IETF)

2. The latest version of the following requirements published by the CA/Browser Forum (https://cabforum.org/) (before this CP/CPS is published):

(1) Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates

(2) Network and Certificate System Security Requirements

(3) Guidelines for the Issuance and Management of Extended Validation Certificates

3、Mozilla Root Store Policy

4、Microsoft Trusted Root Program

5、AATL Technical Requirements

6、Apple Root Certificate Program

7、Chrome Root Program

8、360 Browser Root Certificate Program

9、Oracle Root Certificate

10、WebTrust Principles and Criteria for Certification Authorities - SSL Baseline

1.6.4 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", """"SHALL",

"SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted in accordance with RFC 2119.

The abbreviated time for dates mentioned in this document is 00:00:00 Beijing Time (UTC+8).

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 technical support information on its website https://www.cfca.com.cn. Certificates defined in this CP/CPS will publish certificate log in extension field "Certificate Transparency" (SCT List) to satisfy main Root CA program requirements. It also provides online certificate status query, certificate revocation query services, etc.

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, CP/CPS is updated at least once every 366 days. 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 Access Controls on Repositories

Edit and write access is restricted to only authorized personnel. The information in the CFCA database is available for external query and acquisition in read-only mode.

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.

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 Identity

3.2.2.1 Authentication of Organization Identity

When an institutional subscriber applies for a certificate, CFCA will conduct strict identity authentication, such as verifying the authenticity by querying a trusted database, identifying the identity materials submitted by the applicant, and other methods that can obtain the applicant's clear identity information. The signature (official seal) of the applicant's own or the duly authorized certificate applicant's representative on the certificate application form of the institution-based subscriber shall bear the relevant provisions of the certificate application and the corresponding responsibility.

For all certificates that contain organizational identity information, CFCA verifies the name and registration/business address of the organization. CFCA can perform different authentication methods according to the type of certificate requested by the organization, and the authentication methods refers to the

CA/Browser Forum BR and EVG. CFCA selects one or more of the following items verify the identity and address information of the organization:

1. Based on the following Qualified Independent/Goverment Information Sources, e.g. publicly available records of companies/organizations registries:

- China Organization Data Service
- National Enterprise Credit Information Publicity System
- Ministry of Commerce of the People's Republic of China
- China Corporate Credit Information Service
- China Corporate Credit Information System
- ICP/IP Address/Domain Name Information Filing Managment System

2. An effective document issued by a government agency(including, but not limited to，a business license，a public institution legal person certificate, a unified social credit code certificate, etc.) or by issuing an authoritative third-party database of an effective document to confirm that the organization is a real, legal entity.

3. Obtain the address and contact information of the organization through the trusted third-party database, and contact the organization in the form of telephone, e-mail, postal letter, etc., so as to confirm the authenticity of the information provided by the applicant.

4. Validation of information through certified letters from qualified lawyers，accountants, etc.

5. Confirm the organization's address information through property bills, bank

statements, government-issued tax bills, or other CFCA approved verification methods.

6. The third party is entrusted with the investigation of the organization, or the applicant is required to provide additional information and proof of the material. In addition, if necessary, CFCA also sets up other required authentication methods and data. The applicant has an obligation to ensure the authenticity and validity of the application materials and to bear the relevant legal liability.

CFCA 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

When the user applies for an SSL certificate, CFCA verifies the Applicant's control of the domain name in the certificate applied for. The validation process is

conducted by CFCA and will not be delegated to third parties.

CFCA does not support the validation of domains with .onion as the rightmost Domain Label, and does not issue certificates to such domains.

CFCA maintains a record of the domain validation method used for each domain and the relevant BR version number.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Not applicable.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Not applicable.

3.2.2.4.3 Not applicable. Phone Contact with Domain Contact

Not applicable.

3.2.2.4.4 Constructed Email to Domain Contact

In accordance with the definitions in BR Section 3.2.2.4.4, send a constructed email to domain contact.

Confirm the Applicant's control over the FQDN by

1.Sending an email to one or more addresses created by using "admin", "administrator", "webmaster", "hostmaster" or "postmaster" as the local part, followed by the at-sign ("@") followed by an Authorization Domain Name.

2.Including a Random Value in the email.

3.The Applicant submitting (either by clicking or other means) Random Value to CFCA server to confirm receiving and authorization.

The unique Random Value is generated by CFCA and its validity period is no more than 30 days from its creation. This method is suitable for validating wildcard domain names.

3.2.2.4.5 Domain Authorization Document

Not applicable.

3.2.2.4.6 Agreed-Upon Change to Website

Not applicable.

3.2.2.4.7 DNS Change

In accordance with the definitions in BR Section 3.2.2.4.7, CFCA confirms the Applicant's control over the domain name by confirming the presence of a Random Value in a TXT or CNAME record.

The unique Random Value is generated by CFCA and its validity period is no more than 30 days from its creation.

CFCA uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 when performing validations using this mothod. To count as corroborating, a Network Perspective MUST observe the same Random Value as the Primary

Network Perspective.

Once the FQDN has been validated using this method, CFCA issues certificates for this FQDN and other FQDNs that end with all the Domain Labels of the validated FQDN.

This method is suitable for validating wildcard domain names.

3.2.2.4.8 IP Address

Not applicable.

3.2.2.4.9 Test Certificate

Not applicable.

3.2.2.4.10 TLS Using a Random Number

Not applicable.

3.2.2.4.11 Any other Method

Not applicable.

3.2.2.4.12 Validating Applicant as a Domain Contact

Not applicable.

3.2.2.4.13 Email to DNS CAA Contact

Not applicable.

3.2.2.4.14 Email to DNS TXT Contact

In accordance with the definitions in BR Section 3.2.2.4.14, CFCA sends a verification email to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN, that is "_validation-contactemail". A unique Random Value is included in the verification email.

The Subscriber visits the verification link containing the Random Value and click for approval to complete domain control validation.

The unique Random Value is generated by CFCA and its validity period is no more than 30 days from its creation.

CFCA uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 when performing validations using this mothod. To count as corroborating, a Network Perspective MUST observe the same selected contact address used for domain validation as the Primary Network Perspective.

Once the FQDN has been validated using this method, CFCA issues certificates for this FQDN and other FQDNs that end with all the Domain Labels of the validated FQDN.

This method is suitable for validating wildcard domain names.

3.2.2.4.15 Phone Contact with Domain Contact

Not applicable.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Not applicable.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Not applicable.

3.2.2.4.18 Agreed-Upon Change to Website v2

In accordance with the definitions in BR Section 3.2.2.4.18, the Subscriber puts the specified verification file and a Random Value under the "/.well-known/pki-validation/" directory of the Authorization Domain Name. If CFCA successfully accesses the specified verification contents over the Authorized Port of HTTP/HTTPS protocol, then the Applicant's control over the FQDN is confirmed.

The unique Random Value is generated by CFCA and its validity period is no more than 30 days from its creation. Once the FQDN has been validated using this method, CFCA issues certificates only for this FQDN. This method is not suitable for validating wildcard domain names.

CFCA follow Redirects. Redirects must be initiated at the HTTP protocol layer. CFCA supports the redirects that are the result of a 301, 302 HTTP status code

response. Redirects must be to resource URLs with either the "http" or "https" scheme, and must be to resource URLs accessed via Authorized Ports.

CFCA uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 when performing validations using this mothod. To count as corroborating, a Network Perspective MUST observe the same Random Value as the Primary Network Perspective.

3.2.2.4.19 Agreed-Upon Change to Website – ACME

Not applicable.

3.2.2.4.20 TLS Using ALPN

Not applicable.

3.2.2.4.21 DNS Labeled with Account ID - ACME

Not applicable.

3.2.2.5 Verification Authentication of an IP Address

CFCA accepts Subscribers to apply for SSL certificates using public IP, and public IP is not used to issue Domain Validation and Extended Validation certificates. The IP address used to apply for the certificate must be IANA compliant and cannot be a reserved IP. CFCA maintains a record of the IP validation method used for each IP address and the relevant BR version number.

3.2.2.5.1 Agreed-Upon Change to Website

In accordance with the definitions in BR Section 3.2.2.5.1, the Subscriber puts the specified verification file and a Random Value under the "/.well-known/pki-validation/" directory on the requested IP Address.

If CFCA successfully accesses the specified verification contents over the Authorized Port of HTTP/HTTPS protocol, then the Applicant's control over the requested IP Address is confirmed. The unique Random Value is generated by CFCA and its validity period is no more than 30 days from its creation.

CFCA uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 when performing validations using this mothod. To count as corroborating, a Network Perspective MUST observe the same Random Value as the Primary Network Perspective.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

Not applicable.

3.2.2.5.3 Reverse Address Lookup

Not applicable.

3.2.2.5.4 Any Other Method

Not applicable.

3.2.2.5.5 Phone Contact with IP Address Contact

Not applicable.

3.2.2.5.6 ACME "http-01" method for IP Addresses

Not applicable.

3.2.2.5.7 ACME "tls-alpn-01" method for IP Addresses

Not applicable.

3.2.2.6 Wildcard Domain Names

CFCA verifies the control of the domain name on the right side of the wildcard. The verification rules follow the provisions of Section 3.2.2.4 of this CP/CPS. If the right side of the wildcard domain name is a top-level domain name or a public suffix, CFCA will refuse to issue a certificate for it. CFCA does not issue EV certificates for wildcards.

3.2.2.7 Data Source Accuracy

The data sources used in the forensic process will be published on the official 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 CAA Records

CFCA's policy on CAA records is described in Section 4.2.

3.2.2.9 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

CFCA uses the same set of Network Perspectives when performing Multi-Perspective Issuance Corroboration for the required 1) Domain Authorization or Control and 2) CAA Record checks.

The set of responses from the relied upon Network Perspectives MUST provide the CA with the necessary information to allow it to affirmatively assess:

the presence of the expected 1) Random Value, 2) Request Token, 3) IP Address, or 4) Contact Address, as required by the relied upon validation method specified in Sections 3.2.2.4 and 3.2.2.5; and

the CA's authority to issue to the requested domain(s), as specified in Section 3.2.2.8.

Section 3.2.2.4 and Section 3.2.2.5 describe the validation methods that require the use of Multi-Perspective Issuance Corroboration and how a Network Perspective can corroborate the outcomes determined by the Primary Network Perspective.

CFCA don't reuse or cache the Results or information obtained from one Network Perspective when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives). The network infrastructure providing Internet connectivity to a Network Perspective MAY be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and the CA take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective MAY use a recursive DNS resolver that is NOT co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers MUST be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure

providing Internet connectivity to that DNS resolver.

CFCA MAY immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method (e.g., a CA can immediately retry validation using "Email to DNS TXT Contact" if "Agreed-Upon Change to Website - ACME" does not corroborate the outcome of Multi-Perspective Issuance Corroboration). When retrying Multi-Perspective Issuance Corroboration, CFCA MUST NOT rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

CFCA MAY reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives MAY omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Table: Quorum Requirements

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations
2-5	1
6+	2

The Remote Network Perspectives CFCA uses to perform Multi-Perspective Issuance Corroboration rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

3.2.3 Identification of Individual Identity

If the Applicant's identity is a natural person, CFCA will review the Applicant's name, address, and the authenticity of the certificate application. In the case of a personal identification certificate, CFCA will perform different identity authentication methods based on the different types of certificates applied by the individual. In general, the higher the certificate category, the higher the security level, the stricter the authentication method, and the more comprehensive the authentication content.

The Applicant needs to prove that he or she has control over some of the identity properties contained in the request, such as the e-mail address or domain name involved in the certificate in the certificate request. Applicants may also be required to submit clear copies of valid government-issued documents with photographs (such as identity cards, passports, driver's permits, military officers' certificates or other equivalent documents). CFCA verifies that copies of the documents match the requested names and that other relevant information is correct.

CFCA identifies and validates in one or more of the following ways:

1. The authenticity of the Applicant's certificate request is identified and verified by sending the relevant check code email or by telephone, mobile phone short message and other reliable means. CFCA does not confirm and guarantee the identity information other than the authentication information in the certificate issued is true, reliable and belonging to the Applicant himself.

2. Check whether the copy of the document submitted by the Applicant has any traces of tampering or forgery and, if necessary, verify the identity information provided by the Applicant through reliable means, such as consulting the authoritative third-party database, in order to ensure that the information provided by the applicant is consistent with the results of the verification.

3. Verify the Applicant's address through property bill, bank card statement or credit card bill or rely directly on identity documents issued by the government to confirm the address.

4. When the application information contains organization information. The Applicant may be required to submit a certificate of employment, or query a third-party database, or send a confirmation email to confirm the existence of the organization and whether the Applicant is a member of the organization.

In addition, if necessary, CFCA can also set up other required authentication methods and data. The Applicant has an obligation to ensure the authenticity and validity of the application materials and to bear the relevant legal liability. For Subscriber certificates issued by CFCA, CFCA establishes evaluation criteria to

identify potentially high-risk fraud certificate requests. CFCA can directly reject certificate requests identified as "high risk".

3.2.4 Non-Verified Subscriber Information

CFCA verifies all the information submitted by the subscribers.

3.2.5 Validation of Authority

When an institutional Subscriber authorizes the Applicant's representative to handle the certificate business, CFCA will use the sources listed in Section 3.2.3 to obtain reliable means of communication to verify the authenticity of the Applicant's application.

CFCA can confirm the authenticity of the certificate application directly with the Applicant's representative, or with the department with authority within the Applicant's organization, such as the Applicant's main business office, the company's office, Human Resources Office, Information Technology Office or such other department as CFCA thinks fit.

CFCA also allows the Applicant to provide authorization letters, employment certificates or any equivalent means to verify that it belongs to the above-mentioned institution and that its representative conduct is authorized by the agency. In addition, CFCA allows Applicants to designate independent individuals to apply for certificates. CFCA does not accept any request for a certificate beyond that authorization if the Applicant specifies in writing an independent individual

who can apply for a certificate. Upon receipt of a verified written request from the Applicant, CFCA will provide the Applicant with a list of its authorized personnel.

3.2.6 Criteria for Interoperation

For applications for EV SSL certificates, OV SSL certificates, and DV SSL certificates under the CFCA global trust system, CFCA is responsible for identifying the identity of subscribers and will not entrust other institutions to exercise this responsibility for the time being.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

1. Certificate Reissue

(1) when the subscriber certificate is damaged or lost, e.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.

2. Certificate Renew

Renewal refers to the operation of the subscriber applying for renewal of the certificate within one month before the certificate is about to expire.

Within one month before the expiration of the subscriber's certificate, CFCA will notify the user to renew the certificate through appropriate means.

When renewing EV SSL certificate, OV SSL certificate, DV SSL certificate, the subscriber's identity needs to be re-verified. The verification process and requirements for re-verifying the subscriber's identity are the same as the initial application.

When the renewal operation of EV SSL certificate, OV SSL certificate, DV SSL certificate is successful, the old certificate will be revoked after one month. The renewal of expired certificates does not revoke the old certificate and is processed as a new application. The validity period of the new certificate will be from the date of certificate renewal to the expiration of the original certificate plus one certificate validity period (the validity period of the renewal of an expired certificate is only the validity period of the new certificate).

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 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. The entity should be responsible for any data provided to CFCA by it or the authorized representative.

4.1.2 Enrollment Process and Responsibilities

1. Enrollment Process

(1)Submit a certificate request.

(2) Generating key pairs.

(3) providing the public key (Signed CSR) of the key pair to CFCA.

(4) Agree to the applicable Subscriber Agreement.

(5) Pay any applicable fees.

2. Responsibilities

(1) The Applicant shall know in advance the matters agreed upon in the Subscriber Agreement and this CP/CPS, in particular with regard to the scope of application, rights, obligations and guarantees of the certificate.

(2) It is the responsibility of the Subscriber to provide authentic, complete and accurate certificate application information and material to CFCA.

(3) It is the responsibility of the registration agencies to check and examine the certificate application information and identification materials provided by the Subscriber.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

When CFCA receives the subscriber's certificate application, the CFCA audit team will identify and authenticate the subscriber's identity in accordance with the requirements of Section 3.2 of this CP/CPS. The processing flow is as follows:

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 performed by one person, while the last one must be separated 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 further 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:

① Relying on translation of the materials.

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) CFCA will establish and maintain a high-risk database list of SSL certificates based on certificates that have been denied or revoked for suspected or

identified phishing or other fraudulent purposes, and will query the list information when accepting certificate applications. For Subscribers that appear in the list, CFCA has the right to reject the certificate request or perform additional authentication;

(6) CFCA performs an CAA record check on each DNS Name in the issued certificate subject alias extension and determines whether the certificate application is approved according to the inspection method and results in Section 4.2.4 of the CP/CPS.

(7) Applicant information must include, but not be limited to, at least one Fully Qualified Domain Name (FQDN) or IP address that will be included in the subjectAltName extension of the certificate.

(8) The maximum validity period of subscriber certificates has been clearly defined in Section 6.3.2. CFCA may reuse documents, data, or verification results from previous validations within the following periods, provided that:

• The data sources comply with those listed in Section 3.2;

• The date of data or verification completion is no more than the period specified in the following table from the date of issuance of the current certificate.

Subject Identity Information validation data reuse periods

Certificate issued on or after	Certificate issued before	Maximum data reuse period
-	March 15, 2026	825days

March 15, 2026		398days

For the validation of domain names and IP addresses in accordance with Sections 3.2.2.4 and 3.2.2.5, any data, documents, or completed validation results used must have been obtained within the maximum number of days prior to the issuance of the certificate, as specified in the following table: Domain Name and IP Address Validation Data Reuse Period

Domain Name and IP Address validation data reuse periods

Certificate issued on or after	Certificate issued before	Maximum data reuse period
	2026/3/15	398 days
2026/3/15	2027/3/15	200 days
2027/3/15	2029/3/15	100 days
2029/3/15		10 days

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 the CP/CPS Section 3.2.2. Otherwise, CFCA will reject the request and timely notice the applicant of the result and the reasons.

After CFCA successfully completes verification steps for the certificate application, it means CFCA has approved the certificate application when a formal certificate is issued.

1. Approval of Certificate Applications

CFCA will approve the certificate requests, if the following conditions are met:

(1) The application completely meets the requirements from CP/CPS Section 3.2 regarding the Subscriber's identification information and authentication.

(2) Subscriber accepts or has no opposition regarding the content or requirements of the Subscriber Agreement.

(3) Subscriber has paid applicable fees in accordance with the provisions.

2. Rejection of Certificate Applications

CFCA has the right to refuse the certificate application in case of the following situations:

(1) The application does not meet the specifications of Subscriber's identification and authentication in CP/CPS Section 3.2.

(2) The Subscriber cannot provide the required identity documents.

(3) The Subscriber opposes or does not accept the relevant content or requirements of the Subscriber Agreement.

(4) The Subscriber has not paid or cannot pay the appropriate fees.

(5) The requested certificates contain a new gTLD under consideration by ICANN(The Internet Corporation for Assigned Names and Numbers).

(6) The utilization of the Subscriber's certificate does not comply with the laws and regulations of the place where it is located.

(7) CFCA considers that the approval of the application will bring about controversies, legal disputes or losses to CFCA.

(8) There are some insecure factors such as the length of the public key, algorithm that submitted by the application.

(9) CFCA refuses to issue certificates containing internal names or reserved IP addresses because these names cannot be verified according to Section 3.2.2.2.4 or

Section 3.2.2.5.

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 MAY check CAA records at any time.

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, whichever 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.

For the "iodef" tag, CFCA uses it only for handling compliance reports and notifications, and will not act on its content.

CFCA respects the critical flag, but will refuse to issue certificates for the applicant when encountering unrecognized attributes set in the critical flag.

CFCA uses Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 when performing validations using this mothod. To corroborate the Primary

Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical. Additionally, CFCA MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

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 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.

4.3.1.1 Manual Authorization of Certificate Issuance for Root CAs

Certificate issuance by the Root CA requires an individual authorized by CFCA (i.e. the CA system operator, system officer or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.1.2 Linting of to-be-signed Certificate Content

For SSL Server Certificates, CFCA performs pre-issuance linting to check a tbs Certificate (to-be-signed Certificate) and conducts manual review if an error is found, to prevent mis-issuance that violates BR requirements.

4.3.1.3 Linting of Issued Certificates

CFCA uses Linting tools to test each issued SSL certificate.

4.3.2 Notifications to Subscriber by the CA 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 Subscriber is solely responsible for installing the issued certificate on the Subscriber's computer or hardware security module.

Subscribers are deemed to accept issued certificates, including, but not limited to:

1. Subscribers visit the specialized CFCA certificate service website, and complete downloading the certificate to the digital certificate carrier.

2. CFCA downloads the certificate on behalf of the Subscriber, with the permission of the Subscriber, and sends the certificate to the Subscriber through the security carrier.

3. After the notification of sending the certificate to the Subscriber is received, the Subscriber downloads the certificate through the notice.

4. The Subscriber accepted the manner in which the certificate was obtained and did not object to the certificate or the contents of 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 proactively 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). Subscribers must comply with the requirements of this CP/CPS when using certificates, properly preserve their private keys, and take reasonable measures to prevent the private keys from being lost, leaked, or tampered with. And shall protect their private keys to avoid unauthorized use.

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.

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 paths 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. Confirm that the signature's corresponding certificate is the one trusted by the relying party.

5. Certificate usage is suitable for the corresponding signature.

6. Use certificate's public key to verify the signature.

7. Consider other information specified in this CP/CPS or elsewhere.

If the above conditions are not met, it is the duty of the relying party to refuse the signature information.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

For a Subscriber certificate issued by CFCA, a certificate update may be made from 30 days (inclusive) prior to the expiration of the certificate. As of 30 days(inclusive) prior to the expiration of the certificate, CFCA will notify the Subscriber of the renewal of the certificate by way of a mail notification.

If the Subscriber does not change the certificate subject alias name and the related identity information when the certificate renewal request is submitted, and the verification time of the original certificate does not exceed the period specified in Section 4.2.1 of this CP/CPS, then CFCA verifies the information of the update certificate with reference to the data and the supporting documents verified by the original certificate.

Where the Subscriber needs to change some of the certificate information when submitting the certificate renewal request or the validation limitation of the original certificate has exceeded the time limit specified in Section 4.2.1 of this CP/CPS, the certificate renewal request will be verified in accordance with the process and requirements of the certificate initial application by CFCA.

If the original certificate of the Subscriber has expired, verification in accordance with the process and requirements of the initial application of the certificate is required when applying for the certificate again.

4.6.2 Who May Request Renewal

The entity requesting the renewal of the certificate is a Subscriber or other authorized representative who has applied for a CFCA certificate, and the remaining validity of the certificate is less than 30 days (inclusive).

All subscribers holding certificates issued by CFCA, including individuals, enterprises, institutions, government agencies, social groups, people's groups and other organizations, can request to renew their certificates before their certificates expire.

4.6.3 Processing Certificate Renewal Requests

For certificate update, the processing procedure includes application identification and authentication, certificate information verification and certificate issuance.

1. The identification and authentication of the application shall be based on the following aspects:

(1) The original certificate of the Subscriber exists and is issued by CFCA.

(2) The certificate update request is within the license period.

(3) A Subscriber can submit sufficient information to be able to identify the original certificate, such as a Subscriber's alias name, certificate sequence number, etc.

2. For the processing procedure of certificate information verification, CFCA

will process according to the provisions of Section 3.3.1 of this CP/CPS.

3. CFCA may also choose to verify according to the general initial certificate application process according to the specific application situation of Subscriber certificate update.

CFCA approves the issuance of the certificate only after all the above authentication and verification have been passed.

4.6.4 Notification of New Certificate Issuance to Subscriber

Same as Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Same as Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Same as Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Same as Section 4.4.3.

4.7 Certificate 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

The Subscriber can choose the certificate rekey service when the Subscriber's certificate is as follows:

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. The Subscriber certificate (file) is missing or damaged.

5. Subscriber needs to add domain name (only for multi-domain SSL/TLS server certificate).

6. In case of multiple deployments for a single certificate, the Subscriber needs to use different key pairs.

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

For security reasons, subscribers whose certificates are about to expire should try to update the certificate key to obtain a new certificate.

4.7.2 Who May Request Certification of a new public key

The entity requesting a certificate update is a Subscriber or its authorized representative who has applied for a CFCA certificate and whose certificate has not expired.

All subscribers holding certificates issued by CFCA, including individuals, enterprises, institutions, government agencies, social groups, people's groups and other organizations, can request certificate key update services。

4.7.3 Processing Certificate Re-keying Requests

The processing of certificate key update request is completed by the process of certificate update request in CFCA. See CP/CPS Section 4.6.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

Same as Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Same as Section 4.4.1.

4.7.6 Publication of the Re-keyed 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.

4.8.1 Circumstances for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for the revocation of Subscriber certificates

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 FQDN 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 days.

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.

4.9.1.2 Reasons for the revocation of Intermediate CA certificates

In the event of one or more of the following conditions, CFCA revokes the Intermediate CA certificate within 7days:

(1) The Intermediate CA requests revocation in writing.

(2) The Intermediate CA finds and informs CFCA that the original certificate request was not authorized and does not retroactively grant authorization.

(3) CFCA obtains evidence that the Intermediate CA private key corresponding to the certificate public key suffered a key compromise or no longer complies with the requirements of BR Section6.1.5 and Section6.1.6.

(4) CFCA obtains evidence that the certificate was misused.

(5) CFCA is made aware that the issuance of the intermediate certificate failed to meet the Baseline Requirements, or the Intermediate CA failed to comply with CP/CPS.

(6) CFCA determines that any information that appears in the Intermediate CA certificate is inaccurate, untrue, misleading.

(7) CFCA ceases operations for any reason and has not made arrangements for another CA provide revocation support for the certificate.

(8) CFCA's right to issue certificates in accordance with Baseline Requirements expires, or is revoked or terminated, unless it continues to maintain the CRL/OCSP Repository.

(9) This CP/CPS requires the revocation of the Intermediate CA certificate.

(10) 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).

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 extincted.

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 identify 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 redrawn. 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 redrawn. 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 G2, CFCA OV ECC OCA G2, CFCA DV ECC OCA G2, CFCA EV RSA OCA G2, CFCA OV RSA OCA G2, CFCA DV RSA OCA G2 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 of CRL publication is 24 hours.

4.9.9 On-line Revocation/Status Checking Availability

OCSP service is available for 7*24.

Whether to perform 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.

After the issuance of a certificate or Pre-certificate, the status of the server certificate can be queried via OCSP within 15 minutes.

CFCA provides an updated OCSP response at least 8 hours prior to nextUpdate, and no later than four days after the thisUpdate.

For the status of a Subordinate CA Certificate, CFCA provides an updated OCSP response at least every twelve months, and within 24 hours after revoking the Certificate.

4.9.10 On-line Revocation Checking Requirements

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:

(1) Verify whether signature is compulsory.

(2) Verify the signature using CA Certificate.

(3) Verify whether the certificate is valid or expired.

(4) 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

	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 response is less than 10 seconds. The maximum validity period for OCSP response does not exceed 7 days.

4.9.11 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.

4.9.12 Special Requirements regarding Key Compromise

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

Key compromise can be demonstrated in one of the following ways:

1. Handing over the compromised key to CFCA,

2. Handing over to the CSR named “Proof of compromising the CFCA key” signed with a compromised key

The methods of notifying CFCA about the compromise of key are described in Section 1.5.2 of this CP/CPS.

4.9.13 Certificate Suspension

Not applicable for the certificates under the Global Trust System.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

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. CFCA runs and maintains its CRL and OCSP capabilities with sufficient resources to provide 10 seconds or less response time under normal working conditions.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

The subscription is ended when：

1. The certificate has expired.

2. The certificate is revoked.

4.12 Key Escrow 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.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

Physical and environmental securities of the systems constitute the foundation

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

5.1.1 Site Location and Construction

The computer room of the CFCA CA system is located in the No.2 Building (China UnionPay Beijing Information Center), Zhongguancun Software Park, Haidian District, Beijing. Access to the computer room 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.

The monitoring record file includes all traces in the computer room passage. All CFCA authorized personnel must be accompanied by CFCA personnel when they move in the restricted area. The list of CFCA authorized personnel will be

provided to the CFCA operation department to ensure that only authorized CFCA personnel can enter the computer room. For CFCA visitors who want to enter the computer room, they can only enter after being accompanied by CFCA authorized employees after the corresponding approval.

The certificate service systems of all CFCA authorized service agencies, including registration agencies, acceptance points, etc., must also be protected to ensure that only authorized employees can enter the system for operation. The CFCA administrator is responsible for setting and checking the permissions of the registration agency and acceptance point administrators. The permissions and responsibilities of the registration agency and acceptance point operators are also stipulated in the operation agreement.

5.1.1.1 Public area

The entrance and power distribution of the CFCA site are in this area, and access control measures are adopted. Access cards or fingerprint identification are required to enter.

5.1.1.2 Management Service Area

The service area is the work area for CFCA operators and managers. Two trusted personnel must use access cards and fingerprint identification at the same time to enter. There are logs for personnel entering and leaving the service area.

5.1.1.3 Core Area

The core area is the CA operation and management area. This area must be entered with access cards and fingerprint identification. At the same time, certificate authentication systems, encryption devices and other related password items are also stored in this area. Among them, CA servers, database systems, encryption devices and other related password items are located in the shielded computer room in the core area. The shielded computer room must be entered by two trusted personnel using access cards and fingerprint identification at the same time to ensure that a single person in the shielded area cannot complete sensitive operations. There is a separate buffer zone in the shielded area to prevent electromagnetic wave leakage when the shielding door is opened.

5.1.2 Physical Access

Visitors 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 accompanied 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 break down. A diesel 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 zeroed in accordance with the guidance of the manufacturers. Cryptographic devices and other important key devices are disposed according to the management methods of cryptographic devices.

5.1.8 Off-Site Backup

Currently, CFCA has off-site backup of core data.

CFCA uses offline media to back up key data and audit log data and

transports them to a remote location for storage. The storage facilities meet the description of media storage in 5.1.7.

1. System backup:

CA system performs off-site system backup to prevent the system from not operating normally due to uncertain factors. When the main system cannot operate normally, the backup system will be put into use to continue to provide certification services.

2. Data backup:

CFCA also performs off-site data backup. The operation of off-site backup is specified in the CFCA disaster recovery plan. The security requirements of CFCA off-site data backup media are in accordance with CFCA backup standards and procedures.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles of CFCA include:

Security personnel

Key and cryptographic device management personnel

Cryptographic device operation personnel

System administration personnel

Human resources management personnel

Security auditors

Certificate entry personnel

Certificate identification personnel

CA system developers

Customer service personnel

5.2.2 Number of Persons Required per Task

CFCA has formulated standardized policies to strictly control the division of tasks and responsibilities for the most sensitive operations. For example:

1. Shielded area site access: set to 2 trusted personnel entry and exit mode.

2. Identification, review and issuance of certificates: requires 2 trusted personnel to complete together.

3. Operation and storage of keys and cryptographic devices: requires 3 of 5 trusted personnel to complete together.

4. CA system background operation: requires 2 trusted personnel to complete together.

5. Important system data operation and maintenance: requires at least 1 person to operate and 1 person to supervise and record.

CFCA has a clear division of labor for personnel and implements a security mechanism of mutual restraint and mutual supervision.

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 uses 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 Separation of Duties

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

Security personnel, system administration personnel, network management personnel, subscriber identity and information reviewer, certificate entry personnel, and certificate authentication 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.

5.3.3 Training Requirements

CFCA provides 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 concepts, job responsibilities, internal policies and procedures, certification systems and software, 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 technical 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 punishments according to relevant administration policies and procedures.

5.3.7 Independent Contractor Requirements

CFCA currently does not employ external independent contractors to perform certification-related work.

5.3.8 Documentation Supplied to Personnel

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

In order to ensure the normal and safe operation of the certification system,

relevant documents should be provided to relevant employees, including at least:

1. Certification system operation manual.

2. CP/CPS electronic certification business rules and related protocols and specifications.

3. Internal operation documents, including backup manuals, disaster recovery plans, etc.

4. Job descriptions.

5. Company-related training materials.

6. Related security management specifications.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

1. CA certificate and key life cycle management events:

(1) Key generation, backup, storage, recovery, archiving and destruction.

(2) Certificate request, renewal and re-key request, and revocation.

(3) Approval and rejection of certificate requests, including successful or failed certificate operations.

(4) Cryptographic device life cycle management events, including: device receipt, installation, uninstallation, activation, use, maintenance, etc.

(5) Generation of CRL entries.

(6) Signing of OCSP responses.

(7) Records of introducing new certificate archives and eliminating existing certificate archives.

2. Subscriber lifecycle management events:

(1) Certificate requests, renewals, rekey requests, and revocations.

(2) All verification activities required by the CA/Browser Forum and specified in this CP/CPS.

(3) Acceptance and rejection of certificate requests, including acceptance of subscriber agreements, verification of application materials, storage of application and verification materials, etc.

(4) Issuance of certificates.

(5) Generation of CRL entries.

(6) Signing of OCSP responses.

(7) Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:

1) an identifier that uniquely identifies the Network Perspective used;

2) the attempted domain name and/or IP address; and

3) the result of the attempt (e.g., "domain validation pass/fail", "CAA permission/prohibition").

(8) Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request (i.e., "3/4" which should be interpreted as "Three (3) out of four (4) attempted Network Perspectives corroborated the determinations made by the Primary Network

Perspective).

3. Security events:

(1) Successful and unsuccessful attempts to access the PKI system.

(2) PKI and security system actions performed.

(3) Changes to security profiles.

(4) Installation, update, and removal of software on the certificate system.

(5) System crashes, hardware failures, and other abnormal conditions.

(6) Firewall and router activity.

(7) Entry and exit of CA facilities, including access by authorized and unauthorized personnel and secure storage facilities.

4. System operation events:

(1) System startup and shutdown.

(2) Creation, deletion, setting or modification of system permissions.

(3) Unauthorized access to the CA system network and access attempts.

(4) Unauthorized access to system files and access attempts.

(5) Reading, writing or deletion of security and sensitive files or records.

5. Trusted personnel management records:

(1) Account application records for network permissions.

(2) Application, change, and creation application records for system permissions.

(3) Changes in personnel status.

The above log information includes recording time, serial number, entity

identity of the record, log type, etc.

5.4.2 Frequency of Processing Log

Type one logs listed above are collected and managed by the key administrators; 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

CFCA and its timestamp authority shall retain the following logs for at least two years

1. CA certificate and key lifecycle management event records after the following circumstances occur (as specified in Section 5.4.1(1)).

(1)The CA private key is destroyed.

(2) The CA field in the X.509v3 Basic Constraints extension in the certificate is set to "yes",",",", and the final CA certificate that shares the same public key with the CA private key is revoked or expired.

2. Subscriber certificate lifecycle management event records after the subscriber certificate is revoked or expired (as described in Section 5.4.1 (2)).

3. Any security event records (as stipulated in Section 5.4.1(3)) after the occurrence of an event.

Note: Although these requirements set the minimum retention period, CFCA may choose a longer period to facilitate the investigation and review of potential security incidents or other types of events that may occur.

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 (Internal vs. External)

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

Regarding electronic audit information, CFCA's audit log collection system involves:

1. Certificate management system.

2. Certificate issuance system.

3. Certificate directory system.

4. Certificate acceptance system.

5. Access control system.

6. Website and database security management system.

7. Other systems that need to be audited.

8. Backup and recovery system.

9. User service system.

For paper audit information, there are special file cabinets to collect and archive.

5.4.7 Notification to Event-Causing Subject

When CFCA finds that it has been attacked, it will record the attacker's behavior, trace the attacker to the extent permitted by law, and reserve the right to take corresponding countermeasures. CFCA has the right to decide whether to notify the entity related to the incident.

5.4.8 Vulnerability Assessments

CFCA will conduct a system security assessment at least once a year:

1. Identify foreseeable internal and external threats that may lead to unauthorized access, disclosure, abuse, modification or destruction of any certificate data or certificate management process.

2. Assess the likelihood and potential damage of these threats, taking into account the sensitivity of certificate data and certificate management processes.

3. Evaluate the adequacy of the CA's policies, procedures, information systems, technologies, and other arrangements to address such threats.

5.5 Records Archival

5.5.1 Types of Records Archived

CFCA archives the following:

1. Documents related to the security of the certificate system, certificate management system, root CA system, and entrusted third-party systems.

2. Documents related to certificate requests and the verification, issuance, and revocation of certificates.

5.5.2 Retention Period for Archive

Archived audit logs (as described in Section 5.5.1) will be retained for at least 2 years from their record creation timestamp, or for the period required to be retained in accordance with Section 5.4.3, whichever is longer.

CFCA retains records for at least 2 years including:

1. All archived documents related to the security of the certificate system, certificate management system and root CA system as specified in Chapter 5.5.1.

2. All archived documents related to the verification, issuance and revocation of certificate applications and certificates (as specified in Chapter 5.5.1) after the following circumstances occur:

(1)Such records and documents are finally dependent on the verification,

issuance or revocation of the certificate application and certificate.

(2) The expiration of the subscriber certificate that relies on such records and documents.

If required by law, CFCA will adjust the record retention period. The certificate revocation record in the CRL or OCSP will not be deleted during the validity period of this 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 backed up.

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 (Internal or External)

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 archives. 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:

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

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.

Business interruption is classified as emergencies and disaster 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. Disaster 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 disaster 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, software developers and other third parties with a 7*24 service hotline (400-880-9888) to explain how to report certificate complaints, private key leaks, improper use of certificates, or other forms to CFCA fraud, leakage, misuse or misconduct.

(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.

(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 by official website or other methods. All the certificates will be revoked. No new certificate will be signed with the private key.

1. When a certificate subscriber finds that the certificate private key is compromised, the subscriber must immediately stop using its private key and immediately visit the CFCA Certificate Service Site to revoke its certificate, or immediately notify CFCA to revoke its certificate by phone or email, and reapply for a new certificate in accordance with the relevant procedures. CFCA will publish certificate revocation information in accordance with Section 4.9 of this CP/CPS.

2. When the certificate private key of a CFCA certificate subscriber is compromised, CFCA will immediately revoke the certificate and notify the certificate subscriber; the subscriber must immediately stop using its private key and reapply for a new certificate in accordance with the relevant procedures. CFCA will publish certificate revocation information in accordance with Section 4.9 of this CP/CPS.

3. When the private key of CFCA's root CA or intermediate CA is compromised, CFCA will handle it urgently according to the key emergency plan and promptly notify the relying parties through various channels, such as Microsoft, Mozilla, Google, Apple, Adobe, Oracle, and 360.

5.7.4 Business Continuity Capabilities after a Disaster

CFCA has set up a data backup center and a corresponding BCP to ensure

business continuity 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 Pair Generation

CA key pair 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. A third-party auditor will issue a report indicating that

CFCA's processes and controls in the CA key pair generation process is able to ensure the integrity and confidentiality of the CA key pair. The CA key generation, storage and password cryptographic modules should meet the requirements of the state cryptography administration.

2. RA Key Pair Generation

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

3. Subscriber Key Pair Generation

Generation of subscriber key pairs is performed by the subscribers. CFCA don’t generate key pairs for subscribers. Subscribers should ensure the reliability of the key pairs and is responsible for protecting the private key, and bears corresponding legal obligations.

CFCA rejects subscriber certificate applications that meet the following conditions:

1. The key pair does not meet the requirements of 6.1.5 or 6.1.6 of this CP/CPS.

2. There is clear evidence that the specific method used by the subscriber to generate the private key is flawed.

3. The subscriber's private key has been leaked, if CFCA can deduce the subscriber's private key through a verified method.

4. CFCA has learned in advance that the subscriber's private key has been leaked (for example, through the circumstances specified in 4.9.1.1 of this

CP/CPS).

5. For industry-proven weak private keys. CFCA takes the following precautions for requests submitted on or after November 15, 2024:

(1) In the case of the Debian weak key vulnerability (https://wiki.debian.org/SSLkeys), CFCA rejects all keys found in https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g., RSA, ECDSA) and size listed in the repository. For all other keys that meet the requirements of 6.1.5 of this CP/CPS, except for RSA keys with a size greater than 8192 bits, CFCA rejects Debian weak keys.

(2) In the case of the ROCA vulnerability, CFCA rejects keys identified by https://github.com/crocs-muni/roca or equivalent tools.

(3) In the case of the Close Primes vulnerability (https://fermatattack.secvuln.info/), CFCA rejects weak keys that can be factored within 100 rounds using the Fermat factorization method.

6.1.2 Private Key Delivery to Subscriber

The subscriber's private key is generated by the subscriber himself and will not be transmitted.

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 online platform submission, etc.).

6.1.4 CA Public Key Delivery to Relying Parties

The verification public key used to verify CFCA signatures, including the root CA certificate and intermediate CA certificate of CFCA, can be obtained from the official website of CFCA.

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 G2 —ECC-384（NIST P-384）/SHA-384

CFCA EV ECC OCA G2—ECC-384（NIST P-384）/SHA-384

CFCA OV ECC OCA G2—ECC-384（NIST P-384）/SHA-384

CFCA DV ECC OCA G2—ECC-384（NIST P-384）/SHA-384

CFCA Global RSA ROOT G2 —RSA-4096/SHA-512

CFCA EV RSA OCA G2—RSA-4096/SHA-256

CFCA OV RSA OCA G2—RSA-4096/SHA-256

CFCA DV RSA OCA G2—RSA-4096/SHA-256

The key size of subscriber keys are RSA-2048, RSA-4096 or ECC-256 (NIST P-256).

6.1.6 Public Key Parameters Generation and Quality Checking

CFCA and subscribers must generate public keys in accordance with the provisions of 6.1.1 of this CP/CPS. Public key parameters are generated by compliant devices/platforms to ensure the quality of public key parameters. Public keys must meet the requirements of 6.1.5 of this CP/CPS.

Before issuing a certificate, CFCA will perform public key parameter detection to ensure that the public key parameters meet the following requirements:

For RSA public keys:

1. The public exponent is an odd number greater than or equal to 3.

2. The public exponent range should be between 2^16+1 and 2^256-1.

3. The modulus is an odd number.

4. The modulus is at least 2048 bits and is an integer multiple of 8.

5. The modulus is not a power of a prime number.

6. The modulus has no factors less than 752.

For ECDSA public keys:

The validity of all keys is confirmed by the full ECC public key verification

procedure or the ECC partial public key verification procedure.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The X.509 v3 certificate issued by CFCA contains a key usage extension, which is in accordance with the RFC 5280 standard. For the purposes specified by CFCA in the key usage extension of the certificate it issues, the certificate subscriber must use the key in accordance with the specified purpose.

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

1. Self-signed certificates representing the root CA.

2. Certificates and cross certificates of intermediate CA.

3. OCSP response signing certificates.

The intermediate CA key is generally used to issue the following certificates and CRLs:

1. Subscriber certificates.

2. Timestamp signing certificates.

3.OCSP response signing certificates.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CFCA implements physical and logical protection measures to prevent

unauthorized certificate issuance. For private key backup outside the above-specified verified systems or devices, CFCA stores key fragments in encrypted form in physical devices of different entities to prevent private key leakage. The algorithm used to encrypt the private key fragments and the key length are based on existing technologies and are able to resist cryptanalysis attacks during the remaining life cycle of the encryption key or key portion.

The encryption modules used by CFCA for CA key pairs are all compliant with FIPS 140-2 Level 3 standards.

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

CFCA CA keys are stored in the cryptographic devices, the management key of the encryption machine is divided and 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 generation, update, revocation, backup and recovery of CA private keys use a multi-person control mechanism to distribute the management authority of the private key to five key administrators. The private key can only be operated when at least three key administrators are present and allow it to do so. The administrator IC card must be inserted and the PIN code must be entered.

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. CA key pairs are

encrypted offline during backup and identity authentication is performed before transmission to prevent the loss, theft, modification, unauthorized disclosure, and unauthorized use of CA private keys.

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 CFCA private key is stored in an encrypted form in a hardware cryptographic module that complies with the FIPS 140-2 Level 3 standard.

6.2.8 Method of Activating Private Key

CFCA uses hardware devices (encryption machines) to generate and store CA private keys, and its activation data is divided according to the requirements of CP/CPS 6.2.2. It must be jointly operated by three administrators to complete the activation. Once the CA private key is activated, the activation status will remain until the CA is offline.

6.2.9 Method of Deactivating Private Key

For the CA private key, when the hardware cryptographic module is powered off, reinitialized, or the token/key is removed, the private key enters an inactive state and no unauthorized personnel can perform related operations.

6.2.10 Method of Destroying Private Key

When the life cycle of the CA private key ends, CFCA will archive the CA private key in accordance with the relevant provisions of 6.2.5 of the CP/CPS, and other CA private key backups will be securely destroyed. After the archiving period ends, the archived private key needs to be securely destroyed with the participation of 3 or more trusted personnel.

6.2.11 Cryptographic Module Rating

The cryptographic modules used by CFCA for CA key pairs all comply with the FIPS 140-2 Level 3 standard.

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 validity period of a CA certificate shall not exceed 25 years, and the validity period of an EV/OV/DV SSL certificate follows the table below as BR

required:

Table: Reference for maximum Validity Periods of Subscriber Certificates

Certificate issued on or after	Certificate issued before	Maximum Validity Period
	March 15, 2026	397 days
March 15, 2026	March 15, 2027	199 days
March 15, 2027	March 15, 2029	99 days
March 15, 2029		46 days

The validity period of a CA key pair shall not exceed 25 years. There is no regulation on the validity period of a subscriber certificate key pair.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

1. The activation data of CFCA's CA private key is generated in accordance with the requirements of CP/CPS 6.2.2;

2. For subscribers, the activation data is the password to protect the private key. CFCA recommends that subscribers use a strong password to ensure the security of the private key. The password needs to be:

(1) At least 8 characters.

(2) Contain at least one character and one number.

(3) Contain at least one lowercase letter.

(4) It is recommended that subscribers do not use birthdays, simple repeated numbers, and other information that is easy to guess or crack as passwords.

(5) It is recommended to modify them regularly.

6.4.2 Activation Data Protection

1. CFCA's key managers must protect the secret shares they maintain and must sign an agreement to commit to the responsibilities they assume.

2. For the activation data of CA private keys, CFCA will divide the activation data in a reliable manner and manage it among different key managers.

3. Subscribers must save their private keys in an encrypted form. It is recommended to use two-factor authentication (such as hardware device password enhancement) to protect their private keys.

4. Subscribers' activation data must be properly kept to prevent leakage and theft.

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 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 clients are required to do the same.

6.5.1 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.

CFCA implements multi-factor identity authentication for accounts that can directly export certificate issuance.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

CFCA's development control includes trusted personnel management, development environment security management, product design and development evaluation, use of reliable development tools, etc. The designed production system meets the requirements of redundancy, fault tolerance, and modularity. The software design and development process follow the following principles:

Establish an internal upgrade change application system and require staff to strictly follow the process:

1. Develop the company's internal procurement process and management system.

2. The development program must be strictly tested in the development environment before applying for deployment in the production environment.

3. Perform effective online backup before changing the deployment.

4. Third-party verification and review.

5. Security risk analysis and reliability design.

At the same time, CFCA's system is developed by a reliable developer who

meets the relevant national security standards and has the qualification to produce commercial cryptographic products, and its development process meets the relevant requirements of the national cryptographic authorities.

6.6.2 Security Management Controls

CFCA follows the norms made by the competent department in practicing information security management of its systems. Any system change must undergo 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.

6.6.3 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 backup at the State Cryptography Administration to ensure system continuity.

6.7 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.

6.8 Time-Stamping

Certificates, CRLs, OCSP, and electronic certification service system logs all contain time information, which comes from the country's standard time source.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

In accordance with the requirements specified in RFC5280, the profiles in the following sections cover all certificates issued by CFCA.

7.1.2.1 Root CA Certificate Profile

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

7.1.2.6 TLS Subordinate CA Certificate Profile

7.1.2.7 Subscriber Certificate Profile

7.1.2.8 OCSP Responder Certificate Profile

7.1.2.9 Precertificate Profile

7.1.2.1 Root CA Certificate Profile

See Section 11.1.

7.1.2.1.1 Root CA Validity

See Section 11.1.

7.1.2.1.2 Root CA Extensions

See Section 11.1.

7.1.2.1.3 Root CA Authority Key Identifier

See Section 11.1.

7.1.2.1.4 Root CA Basic Constraints

See Section 11.1.

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

Not applicable.

7.1.2.2.1 Cross-Certified Subordinate CA Validity

Not applicable.

7.1.2.2.2 Cross-Certified Subordinate CA Naming

Not applicable.

7.1.2.2.3 Cross-Certified Subordinate CA Extensions

Not applicable.

7.1.2.2.4 Cross-Certified Subordinate CA Extended Key Usage – Unrestricted

Not applicable.

7.1.2.2.5 Cross-Certified Subordinate CA Extended Key Usage – Restricted

Not applicable.

7.1.2.2.6 Cross-Certified Subordinate CA Certificate Certificate Policies

Not applicable.

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

CFCA issues not only TLS Certificates, but also Document Signing Certificates, and OCSP Responder Certificates. See Appendix 11.2 for the profiles.

7.1.2.3.1 Technically Constrained Non-TLS Subordinate CA Certificate Extensions

See Section 11.

7.1.2.3.2 Technically Constrained Non-TLS Subordinate CA Certificate Policies

See Section 11.

7.1.2.3.3 Technically Constrained Non-TLS Subordinate CA Certificate Extended Key Usage

See Section 11.

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

Not applicable.

7.1.2.4.1 Technically Constrained Precertificate Signing CA Extensions

Not applicable.

7.1.2.4.2 Technically Constrained Precertificate Signing CA Extended Key Usage

Not applicable.

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

Not applicable.

7.1.2.5.1 Technically Constrained TLS Subordinate CA Extensions

Not applicable.

7.1.2.5.2 Technically Constrained TLS Subordinate CA Name Constraints

Not applicable.

7.1.2.6 TLS Subordinate CA Certificate Profile

See Section 11.2.

7.1.2.6.1 TLS Subordinate CA Extensions

See Section 11.2.

7.1.2.7 Subscriber (Server) Certificate Profile

CFCA issues TLS Certificates, see Appendix 11.3 for the profile. In addition, CFCA issues Document Signing Certificates, and OCSP Responder Certificates which are for other usage, see Appendix 11.3 for the profiles.

7.1.2.7.1 Subscriber Certificate Types

The types of TLS Certificates include: Domain Validated (DV), Organization Validated (OV), Extended Validation (EV). Other types include: Document Signing Certificate (DS), and OCSP Responder Certificate.

7.1.2.7.2 Domain Validated

See Section 11.3.

7.1.2.7.3 Individual Validated

Not applicable.

7.1.2.7.4 Organization Validated

See Section 11.3.

7.1.2.7.5 Extended Validation

See Section 11.3.

7.1.2.7.6 Subscriber Certificate Extensions

See Section 11.3.

7.1.2.7.7 Subscriber Certificate Authority Information Access

See Section 11.3.

7.1.2.7.8 Subscriber Certificate Basic Constraints

See Section 11.3.

7.1.2.7.9 Subscriber Certificate Certificate Policies

See Section 11.3.

7.1.2.7.10 Subscriber Certificate Extended Key Usage

See Section 11.3.

7.1.2.7.11 Subscriber Certificate Key Usage

See Section 11.3.

7.1.2.7.12 Subscriber Certificate Subject Alternative Name

See Section 11.3.

7.1.2.8 OCSP Responder Certificate Profile

See Section 11.4.

7.1.2.8.1 OCSP Responder Validity

See Section 11.4.

7.1.2.8.2 OCSP Responder Extensions

See Section 11.4.

7.1.2.8.3 OCSP Responder Authority Information Access

Not applicable.

7.1.2.8.4 OCSP Responder Basic Constraints

See Section 11.4.

7.1.2.8.5 OCSP Responder Extended Key Usage

See Section 11.4.

7.1.2.8.6 OCSP Responder id-pkix-ocsp-nocheck

See Section 11.4.

7.1.2.8.7 OCSP Responder Key Usage

See Section 11.4.

7.1.2.8.8 OCSP Responder Certificate Policies

Not applicable.

7.1.2.9 Precertificate Profile

A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962. A Precertificate appears structurally identical to a Certificate, with the exception of a special critical poison extension in

the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to RFC 5280. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by CFCA that it may issue such a Certificate.

A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate. CFCA will construct and sign a Precertificate corresponding to the Certificate, for purposes of submitting to Certificate Transparency Logs. CFCA will use the returned Signed Certificate Timestamps to then alter the Certificate's extensions field, adding a Signed Certificate Timestamp List, as defined in Section 7.1.2.11.3 and as permitted by the relevant profile, prior to signing the Certificate.

Once a Precertificate is signed, relying parties are permitted to treat this as a binding commitment from CFCA of the intent to issue a corresponding Certificate, or more commonly, that a corresponding Certificate exists. A Certificate is said to be corresponding to a Precertificate based upon the value of the tbsCertificate contents, as transformed by the process defined in RFC 6962, Section 3.2.

CFCA will not issue a Precertificate unless it is willing to issue a corresponding Certificate, regardless of whether it has done so. The Precertificate will be issued directly by the Issuing CA.

The encoded values of the Precertificate Profile are byte-for-byte identical to that of the corresponding Certificate. The fields of Precertificate Profile are the

same as the ones in TLS Certificate Profile as seen in Appendix 11.3. The serialNumber field of the Precertificate is identical to that of the corresponding Certificate. For the extensions of Precertificate Profile, see Section 7.1.2.9.1.

7.1.2.9.1 Precertificate Profile Extensions – Directly Issued

Extension	Presence	Critical	Description
Precertificate Poison (OID:1.3.6.1.4.1.11129.2.4.3)	Must	Y	
Signed Certificate Timestamp List	Must Not	-	
Any other extension	-	-	The order, criticality, and encoded values of all other extensions are byte-for-byte identical to the extensions field of the Certificate.

7.1.2.9.2 Precertificate Profile Extensions –Precertificate CA Issued

Not applicable.

7.1.2.9.3 Precertificate Poison

The Precertificate contains the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3). This extension has an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

7.1.2.9.4 Precertificate Authority Key Identifier

The Precertificate is directly issued by Issuing CA, and the authorityKeyIdentifier extension of the Precertificate is identical to the Issuing CA certificate's subjecyKeyIdentifier.

7.1.2.10 Common CA Fields

Before issuing a certificate, CFCA will ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.10.1 CA Certificate Validity

See Section 11.2.

7.1.2.10.2 CA Certificate Naming

See Section 11.2.

7.1.2.10.3 CA Certificate Authority Information Access

See Section 11.2.

7.1.2.10.4 CA Certificate Basic Constraints

See Section 11.2.

7.1.2.10.5 CA Certificate Certificate Policies

See Section 11.2.

7.1.2.10.6 CA Certificate Extended Key Usage

See Section 11.2.

7.1.2.10.7 CA Certificate Key Usage

See Section 11.2.

7.1.2.10.8 CA Certificate Name Constraints

Not applicable

7.1.2.11 Common Certificate Fields

Before issuing a certificate, CFCA will ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.11.1 Authority Key Identifier

See Section 11.3.

7.1.2.11.2 CRL Distribution Points

See Section 11.3.

7.1.2.11.3 Signed Certificate Timestamp List

If present, the Signed Certificate Timestamp List extension contents is an OCTET STRING containing the encoded SignedCertificateTimestampList, as specified in RFC 6962, Section 3.3.

Each SignedCertificateTimestamp included within the SignedCertificateTimestampList is for a PreCert LogEntryType that corresponds to the current certificate.

7.1.2.11.4 Subject Key Identifier

See Section 11.3.

7.1.2.11.5 Other Extensions

See Section 11.3.

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the subjectPublicKeyInfo field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

CFCA indicates an RSA key using the rsaEncryption (OID:

1.2.840.113549.1.1.1) algorithm identifier, and it is an explicit NULL. When encoded, the AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.

7.1.3.1.2 ECDSA

CFCA indicates an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier.

The parameters use the namedCurve encoding.

For P-256 keys, the namedCurve is secp256r1 (OID: 1.2.840.10045.3.1.7).

For P-384 keys, the namedCurve is secp384r1 (OID: 1.3.132.0.34).

When encoded, the AlgorithmIdentifier for ECDSA keys is byte-for-byte identical with the following hex-encoded bytes:

For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107.

For P-384 keys, 301006072a8648ce3d020106052b81040022.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by CFCA Private Key conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

The signatureAlgorithm field of a Certificate or Precertificate.

The signature field of a TBSCertificate (for example, as used by either a

Certificate or Precertificate).

The signatureAlgorithm field of a CertificateList

The signature field of a TBSCertList

The signatureAlgorithm field of a BasicOCSPResponse.

7.1.3.2.1 RSA

CFCA uses two RSA signature algorithms and encodings:

Signature Algorithm	OID	Hex-encoded bytes
SHA-256 with RSA	1.2.840.113549.1.1.11	300d06092a864886f70d01010b0500
SHA-384 with RSA	1.2.840.113549.1.1.12	300d06092a864886f70d01010c0500
SHA-512 with RSA	1.2.840.113549.1.1.13	300d06092a864886f70d01010d0500

7.1.3.2.2 7.1.3.2.2 ECDSA

CFCA uses two ECDSA signature algorithms and encodings:

Signature Algorithm	OID	Hex-encoded bytes
SHA-256 with ECDSA	1.2.840.10045.4.3.2	300a06082a8648ce3d040302
SHA-384 with ECDSA	1.2.840.10045.4.3.3	300a06082a8648ce3d040303

7.1.4 Name Forms

This section details encoding rules that apply to all Certificates issued by a CA. Further restrictions may be specified within Section 7.1.2, but these restrictions do not supersede these requirements.

7.1.4.1 Name Encoding

For every valid Certification Path (as defined by RFC 5280, Section 6), CFCA applies the following rules:

(1) For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.

(2) For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

When encoding a Name:

(1) Each Name contains an RDNSequence.

(2) Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.

(3) Each RelativeDistinguishedName, if present, is encoded within the RDNSequence in the order that it appears in Section 7.1.4.2, see Appendix B.

(4) Each Name does not contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly allowed in these Requirements.

7.1.4.2 Subject Attribute Encoding

The attributes in TLS/CS Certificates issued by CFCA comply with the requirements for encoding and order in the table below. For other certificates, see Appendix B for the corresponding certificate templates. Subject Distinguished Name Fields (Common Name) contains a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension.

Attribute	OID	Specification	Encoding Requirements	Max Length
countryName	2.5.4.6	RFC 5280	PrintableString	2
stateOrProvinceName	2.5.4.8	RFC 5280	UTF8String or PrintableString	128
localityName	2.5.4.7	RFC 5280	UTF8String or PrintableString	128
organizationName	2.5.4.10	RFC 5280	UTF8String or PrintableString	64
commonName	2.5.4.3	RFC 5280	UTF8String or PrintableString	64

Encoding and order requirements for EV selected attributes are as follows:

Attribute	OID	Specification	Encoding Requirements	Max Length
businessCategory	2.5.4.15	X.520	UTF8String or PrintableString	128
jurisdictionCountry	1.3.6.1.4.1.311.60.2.1.3	EVG	PrintableString	2
jurisdictionStateOrProvince	1.3.6.1.4.1.311.60.2.1.2	EVG	UTF8String or PrintableString	128
serialNumber	2.5.4.5	RFC 5280	PrintableString	64

7.1.4.3 Subscriber Certificate Common Name Attribute

Common Name contains exactly one entry that is one of the values contained

in the Certificate's subjectAltName extension. The value of the field is encoded as follows:

(1) If the value is an IPv4 address, then the value is encoded as an IPv4Address as specified in RFC 3986, Section 3.2.2.

(2) If the value is an IPv6 address, then the value is encoded in the text representation specified in RFC 5952, Section 4.

(3) If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value is encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name are encoded as LDH Labels, and for P-Labels, their Unicode representation will not be used.

7.1.4.4 Other Subject Attributes

See Section 11.3.

7.1.5 Name Constraints

Not applicable.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

See this CP/CPS Section 1.2.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Not applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

Effective 2024-03-15, CFCA issues CRL in accordance with the profile specified as the following.

CRL includes all certificates issued by the CA. If issuing partitioned CRLs, the combined scope of those CRLs is equivalent to that of a full and complete CRL. The CA will not issue indirect CRLs.

Field		Presence	Description
tbsCertList			
	version	Must	v2
	signature	Must	
	issuer	Must	Byte-for-byte identical to the subject field of the Issuing CA
	thisUpdate	Must	The issue date of the CRL
	nextUpdate	Must	thisUpdate. For CRLs covering Subordinate CA Certificates, 12 months after the thisUpdate.
	revokedCertificate	Must	

	extensions	Must	See the table below
signature		Must	

7.2.1 Version Number(s)

CRL issued by CFCA is formatted in accordance with X.509 v2.

7.2.2 CRL and CRL Entry Extensions

Table: CRL Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	Must	N	Byte-for-byte identical to the subjectKeyIdentifier field of the Issuing CA
CRLNumber	Must	N	An integer greater than or equal to zero and less than 2^159, and convey a strictly increasing sequence
IssuingDistributionPoint	*	-	See Section 7.2.2.1

Table: revokedCertificates Component

Component	Presence	Critical	Description
serialNumber	Must	N	Byte-for-byte identical to the serialNumber contained in the revoked certificate
revocationDate	Must	N	For CRLs covering Subscriber Certificates, 7 days after the Normally, the date and time revocation occurred. If CFCA has sufficient evidence to determine that the private key of the certificate was compromised prior to the revocation date that is indicated in the RL entry for that certificate, the revocationDate field will be backdated
crlEntryExtensions	Maybe	-	See the crlEntryExtensions table below

Table: crlEntryExtensions Component

CRL Entry Extension	Presence	Description
reasonCode	Maybe	See the table below for CRLReasons. If reasonCode value is 0, not present; and this reason code is the default option specified in the Subscriber

		Agreement. If reasonCode value is other values, the field presents and is not marked critical.

Table: CRLReasons

RFC5280 reasonCode	Value	Description
unspecified	0	Default option
keyCompromise	1	Indicates that it is known that the Subscriber's private key has been compromised. If there is any other reasons occurred except for key compromise, then reasonCode keycompromise will be used.
affiliationChanged	3	Indicates the Subject's name or other Subject identity information in the certificate has changed
Superseded	4	Indicates that the certificate is being replaced because: the Subscriber has requested a new certificate, CFCA has reasonable evidence that the validation of domain authorization or control for any FQDN or IP address in the certificate should not be relied upon, or the CA has revoked the certificate for compliance reasons such as the certificate does not comply with these Baseline Requirements or CPS.
cessationOfOperation	5	Indicates that the website with the certificate is shut down prior to the expiration of the certificate, or if the Subscriber no longer owns or controls the domain name in the certificate prior to the expiration of the certificate.
certificateHold	6	Not applicable
privilegeWithdrawn	9	Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the certificate Subscriber provided misleading information in their certificate request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

7.2.2.1 CRL Issuing Distribution Point

This extension will not be used when CFCA issues a full and complete CRL.

7.3 OCSP Profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including CrossCertified Subordinate CA Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus must be present.

7.3.1 Vision Number(s)

OCSP V1 version defined by RFC6960.

7.3.2 OCSP Extentions

Consistent with RFC6960.

8 Compliance Audit and Other Assessments

CFCA shall at all times:

1. Comply with the BR and guidelines of the CA/Browser Forum.

2. Comply with the WebTrust audit requirements specified in this chapter.

3. Obtain a CA operating license authorized by the Ministry of Industry and Information Technology.

8.1 Frequency and Circumstances of Assessment

1. Annual Assessment: Conduct a security vulnerability assessment once a year to assess the system, physical site, operation management, etc., and take measures

based on the assessment report to reduce operational risks.

2. Operational Quality Assessment: Conduct an operational work quality assessment once a year to ensure the reliability, security and controllability of operational services.

3. Operational Risk Assessment: Conduct an operational risk assessment once a year to identify internal and external threats, assess the possibility of threat events and the damage caused, and formulate and implement disposal plans based on the risk assessment results.

4. Self-assessment: Conduct a BR self-assessment every year according to the requirements of BR on the CA/Browser Forum.

5. Internal Audit: Perform an internal audit once a quarter and draw at least 3% of the certificate samples.

6. WebTrust Audit: Hire an independent audit firm to conduct an external audit and assessment once a year in accordance with WebTrust's audit specifications for CA.

8.2 Identity/Qualifications of Assessor

The external audit of CFCA is conducted by an organization with the following qualifications:

1. Independent auditing entity.

2. Qualified for WebTrust audit.

3. Must be a licensed and qualified assessment organization with a good

reputation.

4. Understand computer information security system, communication network security requirements, PKI technology, standards and operations.

5. Possess professional technology and tools to check system performance and information security.

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

1. CFCA internal assessment and audit, including:

(1) Whether the CP/CPS, business specifications and security requirements are strictly followed when conducting authentication services.

(2) Service integrity: security management of key and certificate life cycle, certificate revocation operation, security operation of business system, business operation specification review.

(3) Physical and environmental security control: information security management, personnel security control, building facility security control, software and hardware equipment and storage media security control, system and network security control, system development and maintenance security control, disaster recovery and backup system management, audit and archiving

security management, etc.

2.Third-party audit firms perform assessments and evaluations on CFCA to be compliant with CA requirements of WebTrust.

8.5 Actions Taken as a Result of Deficiency

For the issues mentioned in the internal audit report of CFCA, the assessment team will be responsible for supervising related departments' improvements afterwards. After the evaluation from a third-party audit firm had been completed, CFCA will carry out rectification according to the evaluation report, and the second audit and evaluation will be taken.

8.6 Communications of Results

CFCA needs to release the audit report within three months after the end of auditing. If it was delayed more than three months, CFCA will provide explanation document which was signed by a qualified auditor.

The audit report should include the following information that was clearly identified.

1. Name of the organization being audited.

2. The name and address of the organization performing the audit.

3. The SHA-256 fingerprint of all Roots and subordinate CA certificates (including cross-certificates), that were in-scope of the audit.

4. Audit criteria for auditing each certificate (and associated key) (including

version number and associated key).

5. A list of CA policy documents, with version numbers, referenced during the audit.

6. Whether the audit assessed a period of time or a point in time.

7. The start date and end date of the audit period (for those that cover a period of time).

8. The point in time date, for those that are for a point in time.

9. The date the report was issued, which will necessarily be after the end date or point in time date.

CFCA will ensure an authoritative English language version of the publicly available audit information will be provided by the qualified auditor and it is publicly available. The report will be available as a PDF, and is text searchable for all information required. Each SHA-256 fingerprint within the audit report is uppercase letters and does not contain colons, spaces or line feeds.

8.7 Self-Audits

CFCA will conduct continuous self-audits, on at least a quarterly basis, to control the quality of its services. Self-audits are to assess whether the electronic certification activities from the end of the last audit period to the beginning of the current audit period comply with the relevant agreements. CFCA will conduct random reviews of its own electronic certification activities, and the sample size shall not be less than 3% of the total number of certificates issued during this

period.

CFCA uses a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

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.

CFCA will charge Subscriber certification's fees based on the digital authentication service provided. The price standard depends on the regulations of marketing and management departments.

If the price specified in CFCA's agreements with Subscribers is different from the one published, the agreement price shall prevail.

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 only if 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.

3. Audit records include: local logs, server logs, archived logs, which are considered confidential information by CFCA and can only be viewed by security auditors and business administrators. Except as required by law, it cannot be released outside the company.
4. Other personal and company information kept by CFCA should be considered confidential and cannot be published except as required by law.

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. Certificates and the public keys included in the certificates are open, freely queried and verified by users.
3. Information about revoked certificates is public information, and CFCA publishes this information in the directory server.
4. Information related to the application process, application procedures, application operation guide, etc. can be made public. Moreover, CFCA can use this information when processing application business, including publishing the above information to third parties.
5. 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 the privacy of all certificate subscribers' personal information and guarantees full compliance with the relevant national regulations and laws on personal information privacy protection. At the same time, CFCA will ensure that all employees strictly comply with security and confidentiality standards to keep personal privacy confidential.

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. Moreover, such disclosure cannot be regarded as a violation of privacy protection obligations. If such privacy disclosure results in any loss, CFCA shall not be held responsible for it.

9.4.5 Notice and Consent to Use Private Information

1. CFCA uses any subscriber information obtained within the scope of its certification business only for the purpose of subscriber identification, management, and service. When using this information, whether or not it involves privacy, CFCA has no obligation to inform the subscriber and does not need to obtain the subscriber's consent.

2. CFCA has no obligation to inform the subscriber and does not need to obtain the subscriber's consent when disclosing private information to a specific

object under any laws and regulations or at the request of the court or public authority through legal procedures, or with the written authorization of the information owner.

3. Certification authorities and registration authorities must inform subscribers in advance and obtain explicit consent and authorization in a documented form (such as fax, letter, email, etc.) if they intend to use customer's private information for purposes beyond those agreed upon by both parties.

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. Legal application by courts and public authorities when handling disputes arising from the use of certificates.

3. Formal application by arbitration institutions with legal jurisdiction.

4. The subscriber adopts authorization and consent.

5. 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 authorisations have been provided by the subscribers, and shall not be held responsible for the disclosure.

9.5 Intellectual Property Rights

1. 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.

2. CFCA holds ownership, the right of name and the right to share the benefits for certificate system software.

3. CFCA has the right to decide which software system can be used.

4. All the information published at CFCA's website is CFCA's property. Without written permission of CFCA, others cannot repost them for any commercial activities.

5. Certificates and CRLs issued by CFCA are both the properties controlled by CFCA.

6. External operation management strategy and specification are CFCA's properties.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CFCA provides certification services using information security infrastructure 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

information to the CA systems by secure channel.

As the RA, CFCA represents and warrants that:

1. It abides 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

1. Subscriber follow 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 private key and pin code in right ways. The subscriber should be responsible for any mis-use of private key and pin code for any purpose. In case of theft, fraudulent use of a private key and pin code 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 revoke 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:

① Falsehood/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 to fulfil 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 receive 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 paths 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. If the certificate applicant or subscriber provides inaccurate, untrue, or incomplete information and applies to CFCA for the issuance of the certificate, any disputes arising from the subscriber of the certificate shall be borne by the certificate applicant or subscriber themselves, and CFCA shall not be liable or liable for any consequences.

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 because 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

9.9.1 Indemnification scope

If CFCA violated statement in CP/CPS Section 9.6.1, certificate subscribers relying parties and other entities can request CFCA to assume compensation liabilities (except for statutory and contractual exemption). The amount of compensation shall be stipulated by mutual agreement.

If the following circumstances occurred, CFCA will assume limited compensation liability:

1. CFCA issues certificates to a third-party instead of the Subscriber by mistake, which leads to the losses of the Subscriber or relying party.
2. After CFCA knows the fact that Subscriber provides fake registration information or data, CFCA still issues certificate, which leads to relying party suffering losses.
3. If the private key of the certificate is deciphered, stolen or disclosed due to CFCA's fault, which leads to the Subscriber or relying party suffering losses.
4. CFCA fails to revoke certificates in time, which leads to relying party suffering losses.

In addition, CFCA's compensation scope is as follows:

1. All the compensation obligation of CFCA shall not exceed the insurance coverage stipulated in Section 9.2.1. The maximum amount of compensation can be reset by CFCA based on different situations. CFCA will notify related parties immediately after the reset.
2. For the losses caused by subscribers or relying parties, CFCA does not assume responsibilities. Subscribers or relying parties themselves should assume their own responsibilities.
3. CFCA takes the responsibilities only during the validity of the certificate.

9.9.2 Indemnification by Subscribers

If the following situations cause losses to CFCA or relying parties, subscribers shall assume the compensation liability:

1. When Subscribers were applying for certificates, due to deliberate, negligent or malicious provision of false information, which leads to the losses of CFCA or third parties.
2. CFCA and its authorized service agencies or third-party suffer losses due to disclosure and loss of private keys deliberately and by mistake; due to not informing CFCA and its authorized service agencies or third-party of the leakage and loss of private keys with knowing the fact; or due to handing keys to others inappropriately.
3. Subscribers violate the regulations in this CP/CPS and related operation

practices when using certificates as well as using the certificates outside the scope of activities which described in the CP/CPS.

4. If the certificate is used for illegal transactions or causes disputes during the period from revocation requests submitted by the subscribers or other entities authorized by CFCA to this information of certificate revocation published by CFCA. Meanwhile, CFCA operates in accordance with requirements of the CP/CPS, subscribers must assume all responsibilities of losses according to this CP/CPS.
5. Unreal, incomplete or inaccurate information provided by Subscribers.
6. Subscribers continue to use the certificates when information in the certificates is changed and do not notify CFCA and relying parties promptly.
7. The private key is compromised, damaged, stolen, disclosed, etc. due to not taking effective protection measures.
8. Subscribers continue to use the certificate and do not notify CFCA and relying parties promptly when they were made aware that private keys are lost or at the risk of being compromised.
9. The certificate has expired but is still in use.
10. The Subscriber's certificate information infringes upon the intellectual property rights of a third-party.
11. Using Certificated beyond specified scope, such as using certificates for illegal and criminal activities.

9.9.3 Indemnification by Relying Parties

If the following circumstances lead to the losses of CFCA or Subscribers, relying party shall be assumed compensation responsibility:

1. Obligations defined in the CP/CPS and agreements between CFCA and relying parties are not followed.
2. CFCA and its authorized service agencies or a third-party suffer losses due to inappropriate reviews against the CP/CPS.
3. Trust certificates in unreasonable circumstances. For example, relying party still trusts the certificate with knowing that the certificate usage is beyond its scope or period or the certificate has or may have been stolen.
4. Relying party does not verify trust chains of the certificates.
5. Relying party does not check whether a certificate is revoked through querying CRL or OCSP.

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 010-80864610.

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

As authorized by CFCA Security Policy Committee, CP/CPS composition team reviews this CP/CPS at least once a year to ensure that the CP/CPS meets the requirement of national laws, regulations and administration department as well as relevant international standards to ensure it meets actual needs of certification business operations.

Revisions and updates of the CP/CPS should be initiated by the CP/CPS compliance team and approved by CFCA Security Policy Committee. The revised CP/CPS shall be officially released after being approved by CFCA Security Policy Committee.

9.12.2 Notification Mechanism and Period

CFCA reserves the right to amend any term and provision contained in this CP/CPS. And 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 revised CP/CPS.

9.12.3 Circumstances under Which OID Must Be Changed

CFCA decides whether to modify the OID when modifying CP/CPS.

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, the subscriber may file a dispute resolution request with CFCA and notify the relevant parties, or apply for arbitration with the Beijing Arbitration Commission..

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 ClaimAny subscriber or relying party who wishes to file a claim against CFCA shall file it within three years from the date of knowing or should have known of damage to the rights of any subscriber or relying party. If it exceeds three years, 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 (attorneys' fees and waiver of rights)

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 participants are obliged to set up disaster recovery and business continuity plan.

9.17 Other Provisions

CFCA warrants observing the latest version 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 TLS Server Certificates (From http://www.cabforum.org.). Should there be any inconsistency between the CP/CPS and the above Guidelines, the latter shall prevail.

9.18 Final Interpretation Rights

The final interpretation rights of this CP/CPS belong to CFCA, who is responsible for interpretation and revision.

10 Appendix A - CAs constrained by CFCA Global Trust System CP/CPS 4.8

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 G2	ECC-384/ SHA384	CFCA EV ECC OCA G2	ECC-384/SHA384
			CFCA OV ECC OCA G2	ECC-384/SHA384
			CFCA DV ECC OCA G2	ECC-384/SHA384
3	CFCA Global RSA ROOT G2	RSA4096/ SHA512	CFCA EV RSA OCA G2	RSA4096/SHA256
			CFCA OV RSA OCA G2	RSA4096/SHA256
			CFCA DV RSA OCA G2	RSA4096/SHA256

11 Appendix B - Global Trust Certificate Format

11.1 Root Certificate Profile

Multipurpose Root Certificate Field		Critical Extension	Contents
Version			V3
Serial Number			Contain at least 64 bits CSPRNG
Issuer			Byte-for-byte match with Subject
TBSCertificate Signature			CFCA Global RSA ROOT G2: sha512withRSA CFCA Global ECC ROOT G2: sha384withECDSA CFCA EV ROOT: sha256withRSA
Validity: notBefore			The day of certificate generation
Validity: notAfter			25 years
Subject	Common Name (CN)		CFCA Global RSA ROOT G2 CFCA Global ECC ROOT G2 CFCA EV ROOT
	Organization(O)		China Financial Certification Authority
	Country(C)		CN
Public Key Information			CFCA Global RSA ROOT G2 & CFCA EV ROOT : RSA4096 (0ID: 1.2.840.113549.1.1.1) CFCA Global ECC ROOT G2 : secp384r1 (0ID: 1.3.132.0.34)
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier
Extension::subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension:basicConstraints		Critical	Subject Type=CA Path Length Constraint=None
Extension:keyUsage		Critical	keyCertSign,cRLSign

11.2 Intermediate Certificate Profile

Multipurpose PKI Intermediate Certificate Field	Critical Extension	Contents
Version		V3

Serial Number			Contain at least 64 bits CSPRNG
Issuer			Byte-for-byte match the Subject of Issuing CA
TBSCertificate Signature			sha256withRSA sha512withRSA sha384withECDSA
Validity:notBefore			The day of certificate generation
Validity: notAfter			No later than the notAfter of the signing certificate
Subject	Common Name (CN)		See Section 1.1.2
	Organization (O)		China Financial Certification Authority
	Country (C)		CN
Public Key Algorithm			RSA4096 (0ID: 1.2.840.113549.1.1.1) or secp384r1 (0ID:1.3.132.0.34)
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	For Intermediate CA that issues other certificates, the extension is: Policy Identifier=Any Policy (2.5.29.32.0)
Extension: basicConstraints		Critical	Subject Type-CA Path Length Constraint=0
Extension: keyUsage		Critical	digitalSignature, keyCertSign, cRlSign
Extension: extKeyUsage		Not Critical	Must exist. For issuing SSL/TLS types, the extension is: Server Authentication 1.3.6.1.5.5.7.3.1 Client Authentication 1.3.6.1.5.5.7.3.2 For issuing Document Signing Certificates, the extension is: PDF Signing 1.2.840.113583.1.1.5 MS Document Signing 1.3.6.1.4.1.311.10.3.12
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 OCSP AccessMethod=1.3.6.1.5.5.7.48.1
Extension: cRLDistributionPoints		Not Critical	CRL HTTP

11.3 Subscriber Certificate

Format of EV SSL Certificates			
Field	**Value**		
Version	V3		
Serial Number	Contains at least 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 G2 O = China Financial Certification Authority C = CN	CN = CFCA EV ECC OCA G2 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, 2022)	Name of the department (No more OUs from September 1, 2022)
	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 S = 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.
	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	Business Type：one of the following

		Private Organization Government Entity Business Entity Non-Commercial Entity	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	[1]CRL Distribution Point	CRL distribution point of EV SSL	CRL distribution point of EV

Point	Distribution Point Name: Full Name: URL=http://crl.cfca.com.cn/evoca/RSA/crl1.crl	Certificate	SSL Certificate
Key Usage	Digital Signature, Key Encipherment (a0)		
Subject Key Identifier			
Extended 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 at least 20 non-serial digits		
Algorithm	SHA256RSA	SHA256RSA	SHA256ECDSA
Issuer	CN = CFCA OV OCA O = China Financial Certification Authority C = CN	CN = CFCA OV RSA OCA G2 O = China Financial Certification Authority C = CN	CN = CFCA OV ECC OCA G2 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. The Subject's name and/or DBA/tradename. CFCA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, CFCA will documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", CFCA MAY use "Company Name Inc." or "Company Name". If both are	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. The Subject's name and/or DBA/tradename. CFCA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, CFCA will documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name

		included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses.	Incorporated", CFCA MAY use "Company Name Inc." or "Company Name". If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses.
	L = Beijing S = 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.
	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			
Extended Key Usage	Server Authentication (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 at least 20 non-serial digits		
Algorithm	SHA256RSA	SHA256RSA	SHA256ECDSA
Issuer	CN = CFCA DV OCA O = China Financial Certification Authority C = CN	CN = CFCA DV RSA OCA G2 O = China Financial Certification Authority C = CN	CN = CFCA DV ECC OCA G2 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= 2.23.140.1.2.1 [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			
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)		
Subject Alt Name	Public IP or Domain		

11.4 OCSP Responder Certificate Profile

Certificate Field		Critical Extension	Contents
Version			V3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 398 days
Subject	Common Name (CN)		
	Organization (O)		China Financial Certification Authority
	Country (C)		CN
Public Key Information			RSA2048 | 3072 | 4096 or ECDSA P-256 | P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: keyUsage		Critical	digitalSignature
Extension: extKeyUsage		Not Critical	OCSP Signing (1.3.6.1.5.5.7.3.9)
Extension: id-pkix-ocsp-nocheck(1.3.6.1.5.5.7.48.1.5)		Not Critical	0x0500